第3章

新領域と核兵器システム

――核抑止・軍備管理への意味合い――

有江 浩一

航空自衛隊の宇宙作戦部隊訓練の様子（共同）

はじめに

近年、宇宙・サイバー・電磁波などのいわゆる「新領域」での活動が陸・海・空の伝統的な領域での戦いに影響を及ぼしつつあり、また人工知能（artificial intelligence: AI）や量子技術といった新興技術（emerging technologies）が新領域での活動に導入されつつある。これらの新領域での活動や新興技術の影響は核の領域にも及ぼうとしており、核保有国の核兵器システムは従前からのミッションである陸・海・空領域での攻撃の抑止に加えて、新領域での攻撃をいかに抑止していくのかという新たな課題に直面している[1]。

このような課題に取り組む安全保障研究として、「領域横断的抑止」に関するものが挙げられる[2]。この概念は、冷戦後に激変した戦略環境に対応する新たな抑止概念の模索の試みとして2000年代に提唱された「複合的抑止（complex deterrence）」概念が変容したものとされている[3]。カリフォルニア大学サンディエゴ校のガーツキ[4]らによれば、領域横断的抑止とは、ある領域における現状変更的な行動をさせないために、別の領域において脅しを用いること、もしくはいくつかの異なる脅しを組み合わせて用いることだという[5]。ただし、領域横断的抑止は抑止の脅しの信頼性やエスカレーション制御などの面で課題も多い[6]。

領域横断的抑止の観点を含め、新領域での活動が抑止、とりわけ核兵器による抑止にどのような影響をもたらすのかについて、さまざまな見方が提示されている。一方では宇宙・サイバー領域において先制攻撃を行えば（核を含む）何らかの重大な報復を招くことは必至であることから、いかなる国も新領域での攻撃には慎重になるはずだとの見方がある。他方では、宇宙・サイバーなどの新領域における敵対国の活動は核保有国の先制攻撃の誘因を生じさせ、核抑止を不安定化させる恐れがあると懸念されている[7]。また、ある核保有国が新興技術を導入することは、他の核保有国との核抑止関係を不安定化させる潜在的要因になるという[8]。日本国際問題研究所の戸崎は、新興技術が核兵器システムに導入される場合、核保有国間の抑止関係の安定化に寄与するとの見方と、その不安定化を促進するとの見方の双方があると指摘している[9]。

こうした議論を踏まえて、本章では、まず新領域と核兵器システムの関わりを概観し、核兵器システムに対する新領域の影響が核抑止を安定化させるのか、それとも不安定化させるのかを検討する。次いで、新領域の影響が核抑止を不安定化させるとすれば、抑止の安定性を高めるための政策課題は何かを考察する。併せて、新領域における軍備管理のアプローチについても検討を試みる。なお、サイバーや認知領域での戦いにAI技術の導入が検討されるなど、新領域の活動に新興技術が影響を及ぼしていくと考えられることから、本章では新領域と新興技術を併せて論じることとする。

1. 新領域と核兵器システムの関わり

（1）宇宙領域

新領域のうち、宇宙についてはすでに冷戦期から核兵器システムとの関わりが深く、その意味では必ずしも新しい領域ではない。米国の核兵器システムのうち、弾道ミサイルの早期警戒や指揮・通信といった中核的な機能を果たすのは核指揮統制通信（nuclear command, control, and communications: NC3）と呼ばれるシステムであるが、NC3の機能の多くは人工衛星に依存している[10]。これらの衛星は、核のオペレーションのためだけに機能を果たしているのではなく、多くの場合非核（通常）作戦も支援しているのが実態である。このことは核と非核の「もつれ合い（entanglement）」として近年問題視されるようになってきており[11]、宇宙領域と核兵器システムの関わりを考えるうえでも看過できない重要な問題といえる。

衛星をはじめとする宇宙アセットはさまざまな攻撃に脆弱である。宇宙アセットへの攻撃手段である対宇宙（counterspace）システムには、キネティック・物理（kinetic physical）、非キネティック・物理（nonkinetic physical）、電子およびサイバーの各手段がある。キネティック・物理手段は物理的に衛星を直接攻撃するものであり、具体的には地上から発射される直接上昇型ミサイルや宇宙に投入される共軌道（co-orbital）衛星などにより目標衛星を破壊あ

るいは無力化する。非キネティック・物理手段はレーザー兵器や高出力マイクロ波（high-power microwave: HPM）兵器などを使用して目標衛星に物理的影響を与える。電子手段は衛星と地上局間でデータのやりとりを行うための無線電波に対して妨害や欺騙を行うものである。これに対し、サイバー手段は宇宙アセットのデータおよびデータを使用・管理するシステムを標的として攻撃を行う[12]。

現在のところ、キネティック・物理手段のうち直接上昇型ミサイルによる自国衛星の破壊実験を成功させたのは米国、中国、ロシアおよびインドの4カ国であるが、これまでに他国の衛星を攻撃した事例はない[13]。非キネティック・物理手段については、中国が低軌道衛星の光学センサーを眩惑（blinding）または損傷させ得る地上設置レーザーシステムを保有しているとされており、ロシアも同様の能力を有するレーザーシステム「カリーナ（Kalina）」を新たに開発した可能性があると指摘されている[14]。なお、ロシアは限定的な対衛星攻撃能力を持つ地上設置レーザーシステム「ペレスヴェート（Peresvet）」をすでに配備しているとされるが、詳細は不明である[15]。

（2）サイバー領域

宇宙と異なり、サイバー領域は核兵器システムにとって比較的新しい領域といえよう。初期の事例としては、1990年代に米海軍の戦略原子力潜水艦（ship submersible ballistic, nuclear: SSBN）に核ミサイル発射命令を送信するための無線システムに脆弱性が発見され、メイン州にあった海軍の無線送信所が外部のハッカーに乗っ取られそうになっていたことが報告されている[16]。

上記の事例は電磁波領域における電子戦と重なる部分もあるが、兵器体系のコンピュータ化・デジタル化・ネットワーク化が進むにつれて、サイバー領域は電磁波領域と重なり合うようになった。具体的には、ネットワークにつながれたコンピュータは有線あるいは光ファイバーケーブル、マイクロ波、衛星通信などのデジタル通信手段によってサイバー空間にアクセスしているが、これらの通信手段はすべて電磁波を応用したものである[17]。サイバー領域と電磁波領域を介したデジタル情報のやりとりが増えるに伴い、核兵器システムについてもデジタル情報を対象としたサイバー攻撃の脅威が増大している。

当初、核兵器システムへのハッキングは不可能と考えられており、その事案もこれまでに生起してはいない。ただし、サイバーセキュリティの知識を持たない人員やシステム上の欠陥などを狙った攻撃は起こり得る[18]。実際に2020年12月には、核兵器システムそのものではなかったが、米国の核兵器を管理する国家核安全保障局（National Nuclear Security Administration: NNSA）のネットワークがハッキングされたことが明らかになった[19]。また、2022年8月から9月にかけて核関連技術を研究するブルックヘブン、アルゴンヌ、ローレンス・リバモアの3つの米国国立研究所がロシアのハッカー集団「コールドリバー」によるサイバー攻撃を受けた。同集団は、これらの研究所ごとに偽のログイン画面を作って核科学者たちにメールを送信し、彼らのパスワードを窃取しようとしていた。この事案について各研究所はコメントを出しておらず、サイバー攻撃が成功したかどうかは不明である[20]。

核関連施設を標的としたこれらのサイバー攻撃はいずれもインターネット経由で行われたものであるが、インターネットを介さないサイバー攻撃も起こっており、その代表的なものは2010年に公表されたスタックスネット（Stuxnet）事案である。スタックスネットは当時イランのナタンズにあるウラン濃縮施設の遠心分離機の制御システムに感染し、遠心分離機1,000基以上に物理的損害を与えたマルウェアで、インターネットに接続されていない端末にUSBメモリを用いて仕掛けられたとされている[21]。

（3）電磁波領域

すでにみてきたように、核兵器システムは通信をはじめとして電磁波に大きく依存している。このため、電子戦の影響を受けやすく、とりわけ電波妨害（jamming）や電波欺瞞（spoofing）などの電子攻撃（electronic attack）は核兵器システムの機能に少なからず影響を及ぼす[22]。NC3の衛星と地上局間の通信電波のジャミングについては先述したが、これは地上局から衛星に向かう通信（アップリンク）と衛星から地上局への通信（ダウンリンク）のいずれに対しても行うことが可能である。妨害電波を衛星に到達させるために電

力所要が大きくなることから技術的にはアップリンクジャミングの方が難しいとされるものの、一般的には衛星通信に対するジャミングは比較的容易に行うことができコストも高くない。しかも、通信障害が発生した場合、それが意図的なジャミングによるものなのか、それとも電波干渉あるいは混信（interference）によるものなのかを判別しにくいため、攻撃元の特定が困難になるという点も攻撃者にとっては有利である[23]。


ロシア軍の電子戦部隊（Sputnik／共同通信イメージズ）

このほか、電磁波を用いた攻撃に電磁パルス（electromagnetic pulse: EMP）によるものがある。EMPは核爆発などにより放出される強力な電磁エネルギーのことであり、あらゆる電子機器を損傷・破壊し、電力網などの重要社会インフラに広範な被害をもたらす[24]。EMP攻撃に対する核兵器システムの強化策の一環として、米空軍はB-2ステルス戦略爆撃機の対EMP性能を向上させる方策を検討中である[25]。

米国は核爆発によることなくEMPを局地的に放射でき、敵の電子機器を破壊し得るHPM兵器（High-powered Joint Electromagnetic Non-Kinetic Strike Weapon: HiJENKS）を開発中である。HiJENKSは米空軍によるHPM兵器計画（Counter-electronics High-powered Microwave Advanced Missile Project: CHAMP）の成果を基礎として米海軍と共同で開発が進められているもので、最新技術を導入して空対地ミサイル搭載型のCHAMPよりもさらに小型化され、より過酷な環境での運用が可能になるという[26]。なお、CHAMPについては、米空軍は2019年にCHAMP装置を弾頭に搭載した巡航ミサイルを少なくとも20発程度配備したとされる[27]。

レーザーやHPM兵器をミサイル防衛に利用する研究開発も進んでいる。特にレーザー兵器については、米国は将来的に現在の迎撃ミサイルと組み合わせて弾道ミサイルや極超音速ミサイルの迎撃も行えるようなものにするための検討を始めている[28]。さらに、米国防大学（National Defense University）のアンダーソンと米空軍のマッキューは、近い将来に指向性エネルギー兵器を使用して戦域レベルの核搭載可能兵器の誘導システムや通信を機能不全に陥らせ、これらの核兵器を無力化することも可能になるかもしれないと指摘している[29]。

（4）認知領域

認知（cognition）とは、人間の思考プロセスとして定義され、観察による情報の取得、思考、想像、記憶、判断、問題解決、選択的注意（selective attention）といった行為を規定する[30]。人間の認知領域をめぐる戦いである認知戦（cognitive warfare）は、現代戦における新たな領域の1つとみられており、相手（個人レベルと集団レベルの双方）の認知に働きかけてその判断や行動に影響を与える戦い方とされる[31]。その手段としては、ソーシャルメディアを用いた偽情報（disinformation）の拡散などが指摘できる[32]。また、サイバー手段も認知領域での戦いに有効と考えられている。ロシアによる2016年米大統領選への干渉事案では、選挙インフラのセキュリティ上の弱点を狙ったサイバー攻撃が多用された[33]。さらに、電磁波領域の手段が認知領域での戦いに利用される可能性もあり、中国人民解放軍はHPMなどから放射される電磁波により人間の脳を直接攻撃して正常な認知機能を妨害するための兵器を開発中とされている。ある研究者は、こうした攻撃手法を「ニューロストライク（NeuroStrike）」と呼称している[34]。

認知領域と核兵器システムとの関わりでは、2016年に起こった米国の戦術核兵器に関する偽情報の事例が挙げられる。これは同年8月18日、米国がトルコのインジルリク空軍基地に保管している戦術核兵器をルーマニアに移動させたとの報道が世界中に配信され、後にフェイクニュースだったことが判明したものである[35]。ソーシャルメディアが核兵器をめぐる意思決定に及ぼす影響については、対象をツイッター（現X）に絞って考察した研究が2020年に出されている[36]。なお、偽情報の活用によって核使用の事実をどの程度覆い

隠せるかを考察した研究もある[37]。NC3に対する偽情報の影響については戦略国際問題研究所のハースマンが2020年に論文を発表しており、その中でハースマンは偽情報の流布によって米国のNC3に対する国民の信頼が揺らぐ可能性があると指摘している[38]。

核兵器システムをめぐっては、偽情報のみならず誤情報（misinformation）の拡散の事例もある。2017年に中国が新型の地上移動式大陸間弾道ミサイル（intercontinental ballistic missile: ICBM）「DF-41（東風41）」を正式に配備したと複数の大手メディアが写真付きで報じた。しかしその後の調査で、写真はソーシャルメディア上で共有されていたもので、被写体のミサイルとおぼしきものはDF-41とは確認されず、誤情報であったことが判明している[39]。

（5）新興技術の影響

AIや極超音速兵器、量子通信などの新興技術は国際安全保障上の重要な関心事項となっており、これらの技術をめぐって国際的な開発競争が展開されている。新興技術は新領域の動向にも大きな影響を及ぼす可能性があり[40]、また核兵器システムの近代化を進めるうえで大きな期待が寄せられている[41]。

AIは将来的に宇宙領域での戦いに導入される可能性がある。AIの導入によって軌道上の衛星や地上システムの性能が格段に向上するのはもとより、AIの自己学習能力によってアルゴリズム自体が作戦環境に応じて自律的にアップグレードされていくと考えられる。このため、宇宙領域での戦いにAIを導入した側にはかつてないほどの競争上の優位性がもたらされると予測されている[42]。

AIはサイバー領域にも影響を及ぼす可能性がある。将来的にAIによって強化されたサイバー攻撃能力が核兵器システムに指向される場合、核使用の判断を行う短い時間内にサイバー攻撃の探知・識別および攻撃元の特定を完了することは不可能に近くなるとされている[43]。

米国防省が公表した「中華人民共和国の軍事および安全保障の進展に関する年次報告」（2022年）によると、中国人民解放軍が認知領域での戦いにAIの導入を検討しているという。ディープフェイクの作成、プロパガンダの拡散、インターネット利用者の感情の分析にAIを活用するほか、ソーシャルメディア上のボットネットワークにAIを導入してもっともらしいコンテンツを作成させ、最適のタイミングでソーシャルメディア上に投稿させるといった活用法が検討されているもようである[44]。

極超音速兵器の技術は、宇宙を含む領域における新たなキネティック攻撃手段を提供するものとして注目されている。この兵器は、マッハ5以上の極超音速領域で大気圏内を飛翔し、高速飛翔間に機動することが可能であり、現有の防空・ミサイル防衛システムによる迎撃を回避しつつ目標を攻撃できるという軍事的な利点を持つ[45]。極超音速兵器は大気圏と宇宙の境界（ニア・スペース）以下の高度での運用を想定して開発されていることから、航空（air）と宇宙（space）双方の領域にまたがるという特性を有している[46]。ただし、近年ではニア・スペースを超えて宇宙領域で極超音速兵器を活用しようとするかのような動きもある。中国が2021年に実施した新型の極超音速兵器とされる発射試験では、宇宙空間において飛翔体を運搬用ロケットから分離し、地球低軌道に乗せた後に大気圏に再突入させたとみられている[47]。また、米国は極超音速兵器を探知・追跡するためのセンサーを搭載した衛星コンステレーションを地球低軌道に配置する計画を進めている[48]。このように、極超音速兵器とその迎撃手段をめぐる開発競争は宇宙領域にも及びつつある。

中国とロシアが核・非核両用の極超音速兵器を開発・配備しているのに対して、米国は極超音速兵器に核弾頭を搭載する計画を持っていない。リチャード米戦略軍司令官は、こうした非核弾頭搭載の極超音速兵器について、核の敷居を超えることなく戦力を迅速に投射できる新たな攻撃オプションを大統領に付与するものであり、米国の全般的な戦略抑止態勢を強化すると述べている[49]。

量子力学の原理を応用した量子技術（quantum technology）の研究開発が進んでおり、この技術を核兵器システムに導入した場合の影響も論じられつつある。量子技術の導入により、通信や暗号などの秘匿性が飛躍的に改善され、最高レベルの秘匿性を要する核兵器システムの能力向上が期待できるからである。シドニー大学のヘイズによれば、量子暗号通信技術を核保有国のNC3

に導入すれば、傍受・妨害やハッキングが理論上不可能なNC3を構築することができるという[50]。なお、中国は量子暗号通信技術の一方式である量子鍵配送（quantum key distribution: QKD）による実用化を商用ベースで精力的に取り組んでおり、2016年に量子通信実験衛星「墨子号」を打ち上げた。翌2017年には「墨子号」を介して北京とオーストリアのウィーンの間でQKD方式による画像の暗号化伝送を行い、両地点間でのビデオ会議を成功させている[51]。

また、中国は量子レーダーなどの量子センシング技術にも注力している。量子レーダーの軍事的効用は今のところ高くないとみられているが、仮に中国が高性能の量子レーダーの実戦配備に成功した場合は核兵器に対する監視・追跡能力が飛躍的に向上し、米国の核兵器システムに深刻な影響をもたらす可能性があると指摘されている[52]。

2. 新領域が核抑止を安定化させる可能性

(1) 宇宙・サイバー領域における攻撃の相互自制

後述するように、宇宙・サイバーなど新領域における攻撃に対するNC3の脆弱性が多く指摘されているが、攻撃元を特定されないとは限らないため、NC3に対する攻撃を相互に自制するインセンティブが関係国間で働く可能性がある。そもそも、関係国はこれらの領域において先制攻撃を行い、攻撃元を特定されれば何らかの重大な報復を受けることを回避できないと認識しているはずである[53]。ましてやNC3への先制攻撃となれば、核兵器による報復を招く蓋然性が大いに高まることは想像に難くない。

このことを、NC3に対するサイバー攻撃を例に考えてみたい。ロナーガンとヤヒマイロは、こうしたサイバー攻撃を核抑止のシグナリング（核使用を抑止する意思の表明と相手への伝達）の手段として活用できるか検討している。それによると、例えば米国がロシアのNC3に対してシグナリングを目的としたサイバー攻撃を仕掛けようとする場合、ロシアは米国のサイバー手段によるシグナルを自国の重要軍事システムに対する攻撃と解釈し、核抑止の意図とは裏腹に、ロシアによる核使用を招いてしまうという。仮に核使用に至らなかったとしても、ロシアは核戦力の態勢強化や核使用権限の委譲といった核の敷居を下げる措置を講ずるであろうし、それによって偶発的な核エスカレーションの蓋然性が高まってしまう。つまり、サイバー手段であってもNC3に対する攻撃は核抑止を破綻させるリスクが大きいために、米国はこうした攻撃を自制すべきだというのである[54]。

新領域における攻撃の相互自制は米露間のみならず、米中間でも機能するかもしれない。米国防大学のゴンパートとサンダースによれば、米中がともに宇宙・サイバー領域での軍事能力を増大させた結果、これらの領域における攻撃に対して相互に脆弱な状態になりつつあることから、両国がこうした攻撃を相互に自制することはあり得ると分析している。ただし、宇宙・サイバー領域での軍事能力が戦闘における相手の部隊および兵器のパフォーマンスを向上させることを米中ともに理解しているために、これらの軍事能力に対する攻撃オプションを完全に排除することにはならないという[55]。

こうした宇宙・サイバー領域での攻撃オプションが採用されないような措置を講じていくことが、攻撃の自制を維持するためには重要であろう。

電磁波領域での攻撃については、対衛星攻撃手段としては技術的な制約が大きいために自制を余儀なくされることも考えられる。例えば、標的となる衛星と同一軌道に攻撃用の衛星（いわゆる「キラー衛星」）を打ち上げた後、当該衛星に接近させて電磁波攻撃を行わせる状況を検討してみたい。まず、キラー衛星には接近行動に必要な燃料を大量に搭載しておかなければならないが、そのために衛星のサイズと重量が増し、宇宙状況把握のための監視の目を掻い潜りながら隠密に行動することが難しくなる。そうかといって、搭載燃料を多くしつつ衛星を小型化・軽量化しようとすれば攻撃に使用するための電磁波放射装置を搭載するスペースを確保できなくなる。また、電磁波攻撃には大量の電力が必要であり、そのための電力確保も問題となる。太陽光パネルを衛星に付加すれば発見されやすくなり、バッテリーの搭載は衛星の重量を増加させるとともに時間が経つにつれてその消耗が大きくなる。さらに、軌道投入後すぐに接近行動に移行すれば怪しまれることから、攻撃までに年単

位の時間をかける場合もあり、この間に宇宙空間の過酷な環境によりキラー衛星の能力が低下して電磁波攻撃任務の達成が難しくなってしまう恐れもある[56]。これらの技術的なコストの大きさがキラー衛星による電磁波攻撃を自制させる要因となる可能性はある。

新領域における攻撃の相互自制が今後とも続いていくとするならば、抑止論の著名な研究者の1人であったモーガンの「一般抑止（general deterrence）」の概念が示すような状態が継続しているといえるかもしれない。「一般抑止」は、危機発生時における「緊急抑止（immediate deterrence）」とは異なり、危機が発生していない状況での比較的安定した抑止の状態をさす。つまり、抑止国と被抑止国の関係が「一般抑止」の状態にあれば、両者の少なくとも一方は機会があったら軍事力を行使することを考えていたとしても、直ちに攻撃が行われることはないとされる[57]。「一般抑止」は緊急抑止と比べると分析概念として使うには曖昧な点が多いものの、新領域における攻撃の相互自制のメカニズムを抑止の観点から解明するうえで示唆的な概念であろう。

（2）認知領域の活用による核使用の抑止可能性

ハースマンが指摘するように、偽情報の流布によって核保有国のNC3に対する国民の認知に影響を及ぼすことが可能であるとすれば、逆に自国のNC3に対する国民の広範な支持を得ることによって敵対する核保有国に抑止の強い意思を伝達し、敵対国の核使用を抑止する可能性を高めることができるかもしれない[58]。ソーシャルメディア上に可能な範囲でNC3の信頼性についての情報を簡潔かつ理解容易な表現を用いて開示することにより、自国民の支持を集めるように努めるなどの方策が考えられよう。この際、自国のNC3に関して敵対国が偽情報や誤情報を流布してくると思われることから、これらを早期に発見して速やかに訂正するなど適切に対応し、自国のNC3に関する正しい情報が国民に伝わるようにすることが重要である。

また、敵対する核保有国の意思決定者の思考に働きかけ、核使用をめぐる彼らの状況判断と意思決定に影響を与えることによって核使用を抑止しようとすることは認知領域での戦いの一形態として考えられる。米空軍のグーセンは、こうした手法を「認知ターゲティング（cognitive targeting）」と呼称し、核保有国との通常戦争において相手に核使用をさせないように制御しつつ戦争目的を達成する可能性を検討している。グーセンによれば、「認知ターゲティング」とは、軍事力を直接的に相手の国家能力あるいは国家意思の全体に対して用いるのではなく、認知領域において相手の思考を誘導し、自国にとって望ましくないオプションを相手の思考過程から排除させるように間接的かつ焦点を絞って軍事力を運用する考え方である。この際、逃げ道を塞いで相手を追い詰めるのではなく、双方にとって好ましい条件で紛争を終結させる方法として双方が受け入れ可能な（acceptable to both parties as a way to exit the conflict on terms favorable to both parties）行動オプションを提示し、相手がこれを選択するように導くことが重要とされる。そのためには、相手が取り得る行動オプションを含む戦略を早期に洞察し、その裏をかく（outmaneuver his strategy）よう相手に先んじて思考を進めていく必要がある[59]。こうした「認知ターゲティング」によって核使用を抑止するためには、軍事力を相手に対するコミュニケーションの手段として巧妙に運用する必要があり、高度な戦略的思考と軍事力運用の能力が求められるのは言うまでもない。併せて、ソーシャルメディアなどを活用して相手の核使用の誘因を減らすようにすることも考えられる。

（3）新興技術の導入による核使用の抑制

核兵器システムに新興技術を導入することにより、相手国の核兵器システムに対する情報収集・監視・偵察（intelligence, surveillance, and reconnaissance: ISR）能力および収集した情報の分析能力が向上し、核使用の判断をより適正に行うことが可能になるとの見方がある。

ランド研究所のガイストとローンは、NC3の早期警戒システムにAIを導入し、相手国の核態勢に係る動向を正確に把握することができるようになれば、相手国は秘密裏に核攻撃の準備を行うことが難しくなり、相手国による核使用の脅しが本物なのか否か（つまり、核攻撃準備を伴っているのか否か）を正しく見極めることが可能になるため、抑止の信頼性が高まり、危機の際に

偶発的なエスカレーションの危険を減らすことができると述べている[60]。また、コックスとウィリアムズは、AIを核兵器システムに導入することにより、早期警戒情報の分析をより正確に行い得るとともに、核使用の要否を判断するための時間的余裕を得ることが可能になるので、核抑止の安定化に寄与するとみる[61]。

量子技術を応用することにより、相手国の核兵器システムに対するISR能力を向上することも期待されている。例えば、量子センサーは量子効果を利用して磁場や重力、角運動量などのさまざまな物理量を従来のセンサーよりも高感度で計測することができるという[62]。この量子センサーを活用することにより、非脆弱な第二撃能力とされる敵のSSBNの探知が容易になるかもしれない。具体的には、潜航中のSSBNによって引き起こされる磁場や重力などの変化を量子センサーで計測し、探知・追跡に役立てることが考えられる[63]。このようにして、量子センサーによって相手国のSSBNの動向を事前に探知することができるようになれば、相手国による核使用の脅しにも冷静に対応することが可能になり、核使用判断の適正化に寄与するであろう。

新興技術によるISR能力の向上は将来の核軍備管理における検証（verification）を容易にする可能性もある。ISR活動にAI技術を導入し、条約義務の履行状況の監視および検証を強化することにより、条約履行に関する透明性が向上し、信頼醸成に寄与すると考えられる[64]。

3. 新領域が核抑止の不安定化を招く恐れ

(1) 第二撃能力の脆弱化

新領域での攻撃は、第二撃能力を脆弱化させ、核抑止を不安定化させる側面を有する。新領域での攻撃が核抑止に及ぼす影響は、その攻撃が核兵器そのものを標的とするというよりもむしろNC3に対して指向され、NC3を無力化することで核兵器による報復を不可能あるいは困難にし、第二撃能力を脆弱化させることにあると考えられる。例えば、サイバー攻撃によってNC3の早期警戒システムが攪乱される、通信が遮断されて核攻撃命令を受信できなくなる、もしくは核運搬システムのソフトウェアが破壊されて発射できなくなるといった事態は、核保有国の第二撃能力を脆弱化させるであろう[65]。

また、NC3へのサイバー攻撃を皮切りに、新興技術を駆使した第二撃能力への対兵力打撃を行うとのシナリオも考えられる。例えば、中国あるいはロシアが、まずサイバー攻撃で米国のNC3の機能を停止させた後、極超音速兵器でICBM発射基地を壊滅させ、水中ドローンと先進型センサーで米SSBNを捕捉撃滅する、というシナリオを米大西洋評議会のパベルとトロッティが提示している。それによると、米国が残存核戦力で報復攻撃を行ったとしても、中国あるいはロシアの先進型防空ミサイル防衛網ですべて撃破されてしまうため、米国の核抑止力は無力化されるという[66]。このように、もしNC3へのサイバー攻撃が行われてNC3が機能不全に陥った場合は、核保有国の第二撃能力は対兵力打撃に脆弱となろう。

次に、新興技術の影響を検討してみたい。概してAIや極超音速兵器などの新興技術は、核兵器を探知・追跡し、これを精密に打撃して破壊する能力を向上させ、第二撃能力の脆弱化に寄与することで核抑止の不安定化を招くものと考えられる。イェール大学のブラッケンは、AIなどの新興技術の導入によって核保有国の第二撃能力、特に地上移動式の核ミサイルを容易に探知・追跡できるようになると、核抑止が不安定化すると論じている。危機の際に核保有国は、AIなどで強化された敵のISRシステムで探知・追跡されないようにするために核ミサイルを移動・分散しようとするであろう。そうした動きを核戦争も辞さないというシグナルだと他の核保有国が誤解してしまうことによって、第一撃の誘因を与えることになりかねないという。また、AIの導入による第二撃能力の脆弱化を恐れた核保有国が核戦力の増強に乗り出し、核軍備競争を引き起こすリスクもあるという[67]。中露の第二撃能力は地上移動式核ミサイルを主体としていることから、こうした影響を受けやすいと考えられる。

さらに、米国の非核極超音速兵器によって中露の第二撃能力が脆弱化される可能性も指摘されている。ジョンズ・ホプキンス大学のウィルケニングは、米国の極超音速兵器が中露の地上移動式ICBMに到達し得る十分な射程を有するに至った場合は、両国のICBMは脆弱化するであろうと指摘する。ただし、

中露の報復攻撃による損害を米国が相当程度限定できない以上、両国に対して米国が非核極超音速兵器による先制攻撃を行う誘因は非常に少ないという[68]。

戦略的安定は、敵対国が自国の核抑止力を毀損し得ないと確信できている状態[69]とされることから、新興技術によって核抑止力（第二撃能力）の残存性が脅かされれば戦略的安定は動揺することになる。新興技術を導入した敵対国による武装解除のための第一撃を恐れる核保有国は、攻撃によって自国の第二撃能力を喪失する前に核を先行使用しようとするかもしれない。つまり、自国の第二撃能力が脆弱化すると認識すれば、当該国は核戦力を早期に使用しなければならないとの衝動に駆られ、危機の際に第一撃の誘因が高まるのである。ジョージタウン大学のクローニグは、こうした「use it or lose it」のロジックを強調しすぎることを戒めつつも、このまま中国やロシアなどの現状変更国に新興技術が拡散していけば非核（通常）戦争のリスクが高まり、ひいては核エスカレーションが生起して戦略的安定を揺るがしかねないと分析している。その一方で、米国をはじめとする現状維持国にとって新興技術は既存の戦略的安定を強化するものになるとの見方を示している[70]。

量子技術も第二撃能力の脆弱化を促進する恐れがある。先述したように、量子センサーによってSSBNの探知・追跡が容易になれば、SSBNの非脆弱性が大きく低下し、核抑止の不安定化を招来するであろう。また、量子技術がAIと結び付き、量子コンピューティングによって強化されたAIが搭載された場合、極超音速兵器をさらに迎撃困難なものにするとの指摘もなされている[71]。

サイバー領域にAIが導入されることにより、SSBNがサイバー攻撃によって脆弱化される恐れもある。アバディーン大学政治・国際関係学部のジョンソンは、サイバー攻撃の一種である「高度標的型攻撃（advanced persistent threat: APT）」にAIを活用して攻撃を自律的に行わせることにより、SSBNのようなサイバーセキュリティの高い標的に対してもセキュリティ上の弱点を高速度で見つけ出して侵入することが可能になるかもしれないと警鐘を鳴らしている。そうした攻撃の機会としては、SSBNが整備のためにドック入りしている時が挙げられるという[72]。

このように、新領域・新興技術が第二撃能力を脆弱化させるリスクが高まっていることから、第二撃能力のレジリエンス（抗たん性）を高めて拒否的抑止、つまり第二撃能力への攻撃を阻止する態勢を整え、攻撃の目的を達成できないと思わせることで攻撃を断念させる抑止の方策が求められる。特に、NC3は新領域での攻撃に脆弱であるため、拒否的抑止の態勢を強化することは喫緊の課題であろう。米エアロスペース・コーポレーションのグリーソンらは、宇宙アセットのレジリエンスを高めることによって敵に攻撃を諦めさせ、抑止を強化すべきだと主張している。レジリエンス強化の方策としては、デコイ衛星や護衛手段を配備するほか、衛星の数を増やすことなどを挙げている[73]。

しかし、NC3への攻撃に対して拒否的抑止を強化することには限界がある。一般に衛星を攻撃から守る方法には、衛星を堅牢化する（hardening）、機動性（maneuver）を強化する、護衛用のアセットを軌道上に配備するなどが考えられる。このうち、堅牢化と機動化については衛星の発揮すべき性能（監視能力や通信能力など）および設計寿命とトレードオフの関係にあり、通常は衛星を設計する際に性能を最大化することが求められるため、これらの自己防御機能は縮小せざるを得なくなる。また、護衛用のアセットも今のところは技術的に難しい[74]。よって、宇宙での対衛星攻撃について拒否的抑止を強化することには技術面で限界がある。

NC3に対するサイバー攻撃への拒否的抑止も実際には難しい。一般に標的となっているシステムのサイバーセキュリティを防御側が向上させることにより、攻撃にコストがかかり、そのコストに見合うだけの成果を得られないと攻撃側に思わせることができれば拒否的抑止はある程度強化できるが、サイバーセキュリティの向上には大き

高まるサイバー攻撃の脅威（Jonathan Raa／NurPhoto／共同通信イメージズ）

な人的・技術的・財政的コストがかかる。その反面、攻撃側は標的システムのセキュリティ上の弱点を発見して侵入すればよく、防御側が侵入に気づいて弱点を修正してくれれば他の弱点を探せばよいだけであり、攻撃のコストは小さい。これに対して、防御側がいかにコストをかけようとも、システムが有するすべてのセキュリティ上の弱点を事前に発見して修正しておくことは不可能である[75]。NC3のシステムは最高レベルのサイバーセキュリティを求められるとはいえ、セキュリティ上の弱点を皆無にすることはできない。米議会は、米国のNC3のサイバーセキュリティを向上させるため、国防省に対して必要な措置を求める関連法案を矢継ぎ早に通過させている[76]。しかし、NC3のサイバーセキュリティの向上には通常の兵器システム以上に大きなコストがかかると予想されることから、NC3へのサイバー攻撃によって達成され得る利得を上回るコストを攻撃側に賦課し、攻撃を行う誘因を減少させ得るほどにNC3のセキュリティレベルを引き上げられるかどうかは疑問が残る。

(2) 新領域での攻撃に対する懲罰的抑止の実効性の問題

前項で検討した新領域・新興技術による第二撃能力の脆弱化は、攻撃すれば確実に報復されるとの被抑止側の確信を揺るがすことになり、懲罰的抑止の実効性を低下させる。そもそも、懲罰的抑止が成立するには、抑止側が攻撃元である被抑止側を特定できることが前提となる。しかし、新領域での攻撃においては、攻撃元を特定すること自体が難しい。宇宙領域においては、軌道上の物体を観測するための宇宙監視レーダーや望遠鏡のカバレッジには多くの死角があるため[77]、衛星に対する何らかの攻撃が行われたとしても、攻撃元の特定に至る詳細な情報を得ることは困難である。対衛星攻撃用の直接上昇型ミサイルであればセンサーによる探知・追跡情報から発射位置を突き止め、ミサイルを発射した国を特定することは可能であるが、レーザー兵器や電子戦による対衛星攻撃の場合は探知・追跡自体が難しく、攻撃元の特定には相当な困難を伴う[78]。サイバー領域においても、サイバー攻撃の発信源を特定するに足る十分な証拠を集めるには数カ月かかるとされており、抑止のための効果的な対応を行う時機を失してしまう[79]。

たとえ攻撃元を特定できたとしても、攻撃に対して耐え難い報復を加えると攻撃側（被抑止側）に確信させることが新領域では困難な場合がある。宇宙領域の場合、衛星は無人のため、それを攻撃したとしても人的被害が生じないことから、必ず報復が実行されると攻撃側（被抑止側）が確信するとは限らないかもしれない。また、先述したように対衛星攻撃手段にはキネティック・物理、非キネティック・物理、電子およびサイバーの4類型があり、それぞれの手段を活用した具体的な攻撃オプションは回復可能な（reversible）一時的機能不全をもたらすものと回復不可能な（irreversible）永続的損害を与えるものを含めて数多く存在する。これらすべての攻撃に対して抑止上有効な報復手段を揃えることは不可能に近いため、各攻撃に対する明確で具体的な信頼性ある（clear, specific, and credible）抑止の脅しを抑止側が発出することが難しくなる。そうなると、懲罰的抑止が不確実な状況が生起し、その状況は敵に攻撃の誘因を与えることになる。例えば、彼らは非キネティック手段による攻撃を試しに行って抑止側の報復意思をテストしてくるかもしれず、こうした攻撃を許すこと自体が抑止の失敗といえよう[80]。

では、宇宙領域における報復のための対衛星攻撃手段を軌道上に配備し、同種の報復を行える態勢を整えればよいのかというと、対衛星攻撃システムの宇宙配備をめぐる国際的な軍備拡張を引き起こすことになるために難しいであろう。元駐ヨルダン米大使のハリソンらは、米国が対衛星攻撃への対応を宇宙における同種の報復に限定することは抑止上不利になるとして、他の領域における比例性を欠いた対応（disproportional response）の可能性も排除できないと攻撃側に思わせることが抑止の不安定化を緩和するであろうと示唆している[81]。

サイバー領域の場合、攻撃元を特定できたとして、サイバー攻撃を行った側（被抑止側）のネットワークシステムに対してサイバー手段による同種の報復攻撃を行うことには技術的な困難が伴う。抑止側がサイバー手段による報復の脅しを発出することは技術情報を漏らすことにつながり、被抑止側が自己のネットワークシステムの脆弱性を修正するための機会を与えてしまうことになりかねない。また、分散型サービス拒否（Distributed Denial of

Service: DDoS）攻撃による報復についても、DDoS報復攻撃が差し迫っていることを被抑止側が知り得た場合、防護すべき重要なシステムをネットワークから切り離す、または有害なネットワークトラフィックをリダイレクトするなどの対応措置を講ずることで無効化されてしまう。セキュリティ上の対策が講じられていない未知の脆弱性を突くゼロデイ攻撃による報復については当初こそ有効性があるものの、報復を実行すれば被抑止側が脆弱性を発見して修正プログラムを適用するために有効性は失われてゆく[82]。

サイバー攻撃に対して核兵器による報復を行うことは、その攻撃が米国のNC3を含む主要な核兵器システムを無力化させるような重大なものであった場合に信憑性を帯びる[83]。したがって、サイバー攻撃に対して核報復の脅しによる抑止を図ることは可能と思われる。しかし、その脅しが著しく比例性を欠いているために信憑性が低いと攻撃側が判断した場合は、核兵器の抑止力が損なわれる恐れがある。また、核の脅しが功を奏さず、サイバー攻撃が実行されてしまった場合にどうするのかという問題もある。NC3に対するサイバー攻撃への対応をめぐる国内からの弱腰批判に反論するとともに、核の脅しの信憑性に係る国際的な認識を高めるためにも核兵器使用を命じなければならないといった意思決定者の心理的圧力が増大する中で、核へのエスカレーションのリスクが高まり得ることも留意しておく必要がある[84]。

（3）意図せざる核使用の可能性の高まり

新領域での攻撃が攻撃側の意図しない形でエスカレーションを起こし、あるいは被攻撃側の誤認によって核兵器が使用されかねない事態に発展する可能性が高まっている。特に、米中露の3カ国は相互のNC3を標的とし得る対宇宙能力やサイバー攻撃能力を高めつつあり、これらの能力による自国のNC3への奇襲攻撃が戦略的安定を損なうとの認識を互いに共有している。国際危機の際には、3カ国の軍隊は自国の核兵器システムに対する攻撃の兆候を見逃すまいと監視態勢を強化するであろう。こうした状況下で、米中露が関わる局地的な通常戦争が生起した場合、通常作戦を自国に有利に進めようとして相手国の通常作戦を支援しているC3システムを標的とする対宇宙あるいはサイバー手段による攻撃が行われることが考えられる。しかし多くの場合、米中露の通常作戦用のC3システムはNC3と両用となっている[85]。このため、意図的にNC3を外して通常作戦用のC3システムだけを攻撃しようとしても、結果的にNC3への攻撃となってしまうことで、核へのエスカレーションを招くリスクが高まることになる。例えば、米国のNC3を支援する軍事用衛星のうち、どれがNC3用でどれが通常作戦用なのかは判然としていないのである[86]。

新領域での攻撃に対して核保有国の第二撃能力が脆弱化する可能性もまた、意図せざる核兵器使用のリスクを高める。アクトンは、核兵器システムがサイバー攻撃に対して脆弱であるために意図せざる核エスカレーションのリスクが生じると述べている。核兵器システムに対して直接指向される対兵力的サイバー攻撃はもとより、核兵器システムの情報窃取を目的として行われるサイバースパイ活動（cyber espionage）もこうしたリスクを引き起こす。たとえ情報窃取を目的としたサイバー活動だと被攻撃国が判断したとしても、被攻撃国はその活動によって収集された情報が自国への対兵力打撃に使用され得ることを懸念するであろう。そもそも、サイバースパイ活動と通常のサイバー攻撃とを迅速に判別するのは困難であるため、核兵器システムに対するサイバースパイ活動は（対兵力的）サイバー攻撃と誤認されるリスクが高い[87]。特に、NC3に対してサイバー攻撃を受ければ、自国の核兵器システムが無力化される前に紛争をエスカレートさせ、核兵器を使用しなければという重圧が被攻撃国にのしかかるため[88]、意図せざる核エスカレーションを招きやすい。

認知領域での戦いにおいて、米軍が「ニューロストライク」兵器の脅威に直面し[89]、核抑止を不安定化させる可能性もある。この兵器による人体への攻撃は、ともすれば単なる健康被害と判断されてしまうために攻撃を探知することが困難であり、抑止が効かないと考えられている[90]。「ニューロストライク」兵器を手にした核保有国は、同兵器によって核使用に関する意思決定者の判断に影響を与え、自国に有利な状況を作り出そうとするかもしれない。ただし、「ニューロストライク」兵器の有効範囲は限定的であり、意思決定者を対象とした攻撃は難しいと思われる。仮に可能であったとしても、相手の認知を思

いどおりにコントロールできるわけではないため、意図しない判断を招いて核抑止が破綻するリスクが大きい。

新興技術が核兵器システムに導入されていけば、誤解、誤認、誤算あるいは事故などによる意図しない核兵器使用のリスクが高まると懸念されている[91]。こうした懸念が高まった背景には、ロシアによる無人水中核兵器の開発計画（ロシア側呼称は「海洋多目的システム　ステータス6」）の存在が世に知られ、その兵器にAIが搭載されていると分析されたことがある[92]。後に「ポセイドン」と名付けられたこの無人核兵器に実際にAI技術が適用されているとすれば、危機における予測可能性が低下し、相手の意図を誤解するリスクが高まりかねない[93]。

「ポセイドン」のケースは核兵器そのものにAIが導入された事例であるが、核抑止を不安定化させる点でより深刻なのはNC3へのAIの導入である。AIはNC3の通信、早期警戒システム、意思決定支援、報復攻撃の自動化の4分野に導入されると考えられるが[94]、このうち特に論争的なのは意思決定支援と報復攻撃の自動化である。意思決定支援については、AIが意図しない行動をもたらし、偶発的な核戦争にエスカレートするリスクを高めることが懸念される[95]。また、報復攻撃の自動化では、ロシアがソ連時代に整備したとされる自動核報復システムが例として挙げられる。これは、核攻撃を受けてロシアの指導部が壊滅する事態に備えたシステムで、核爆発の兆候となる地震波などをセンサーが感知すると、指導部の生存を確認できなかった場合は半自動的に核ミサイルによる報復攻撃を発動する仕組みになっている[96]。ランド研究所のバレットは、ロシアの自動核報復システムのセンサーが隕石の衝突を米国の核攻撃と誤認する可能性があり、これによって意図しない核使用が行われるかもしれないと指摘している[97]。

また、認知領域での攻撃がNC3に実装されたAIに影響を及ぼす場合、意図しない核エスカレーションのリスクが高まる恐れがある。例えば、AIのアルゴリズムによって紛争の進展速度が増大する中、核保有国のAIシステムに偽情報が仕込まれていることが考えられ、それが意図しないエスカレーションを生起させる可能性があるという。このため、NC3に実装されたAIに偽情報やディープフェイク、意図的に操作されたデータなどが仕込まれるケースを想定して、これらを識別するための技術的措置を研究しておく必要性が指摘されている[98]。

NC3へのAI導入に伴うさまざまな問題点に鑑みて、AIの導入にあたっては運用上・技術上のあらゆる措置を講じるべきだとの議論や、あるいは導入を見送るべきだとする議論が提起されている。この問題に詳しい研究者であるラウテンバッハは、AIに起因する偶発的な核使用を防止するためには、AIが下す判断に人間が介在すること（human-in-the-loop）はもちろんのこと、そのほかにもNC3へのAI導入にあたって実行可能な技術的解決策を講じておくとともに厳正な技術審査を行うこと、さらには核ドクトリンや核政策の変更といった核運用に係る抜本的な措置が求められるとしている[99]。また、ヨーロピアン・リーダーシップ・ネットワークのサルティーニは、AIをNC3に実装するのは技術的に時期尚早であるため、これを一時的に停止する措置（moratorium）が必要であり、まずは核兵器国5カ国（米英仏中露）がその実現に向けた協議を開始すべきだと指摘する。そのうえでサルティーニは、ゆくゆくは印パなど他の核保有国を協議に参加させ、すべての核保有国が一時停止措置に合意することができれば望ましいと述べている[100]。

4. 今後の課題と展望

(1) 新領域による核抑止の不安定化への政策課題

これまでの考察において、新領域と核兵器システムとの関わりが核抑止を安定化させる可能性があると同時に、核抑止の不安定化を招く恐れもあると論じてきた。ここで、前者の核抑止を安定化させる可能性について、もう少し検討してみたい。

まず、宇宙・サイバー・電磁波領域における攻撃の相互自制であるが、特にNC3に対する攻撃は核報復を招く可能性が高いため相互に自制することが想定し得る。ただし、こうした相互自制を成立させることはけっして容易ではない。

抑止の脅しは、抑止しようとする行動に対して比例的（proportionate）とみなされる場合に信頼性があると認識される。この点で、NC3に対するサイバースパイ活動を抑止しようとして核報復の脅しを用いることは信頼性があるとはみなされないであろう[101]。

その一方で、攻撃を企図する国（被抑止国）は相手国が必ずしも比例的な報復に限定してくるとは確信できないはずである。例えば、宇宙での対衛星攻撃に米国が同種の報復で応じるにとどめることは、米国を（抑止上）不利な立場に置くものと考えられる。このため、攻撃国はその攻撃に対して米国が比例性を欠いた報復行動で応じ、急速なエスカレーションを招いてしまう可能性を考慮に入れざるを得ない[102]。これは危機の際に相互の緊張を高め、エスカレーションが起こりやすくなることを意味する。こうした状況に陥るかどうかは、新領域をめぐる被抑止国とのコミュニケーションの度合いによるであろう。

次に、認知領域の活用による核使用の抑止可能性、特に「認知ターゲティング」については、自国の戦略を相手に見破られた場合は機能しない。この場合、相手は認知バイアスを誘発させて、相手の行動を読み違えさせるか、あるいは自国の対応行動に疑問を抱かせるなどしてその抑止戦略を破綻させようとするであろう。例えば、自国の抑止戦略が功を奏しているとの楽観主義バイアス（optimism bias）を促進させる、あるいはその逆に、抑止がすでに一部破綻しているとの偽情報を流して混乱を引き起こす、などが考えられる[103]。こうなると、認知領域での戦いにおいて相手に主導権を握られてしまい、相手による偽情報の流布などを通じた認知操作を受けて合理的な思考が歪められれば、核抑止が破綻するリスクが高まる。

最後に、新興技術の導入による核兵器使用の抑制については、核保有国のうち新興技術を先に導入した側には抑制効果があると思われるが、技術が拡散して相手国も導入した場合は逆に核抑止の不安定化を招くことになりかねない。例えば、NC3にAIを導入すれば意思決定者にとって核使用判断の時間的余裕を得ることができるであろうが、自国のみならず相手国も導入している場合は双方ともにAIによって判断時間が短縮される状況が生起し、事態の進展速度が一段と早められることになる[104]。

これらの検討から、新領域と核兵器システムとの関わりが核抑止を安定化させる可能性はあるものの、その可能性は新領域をめぐる被抑止国との関係あるいはコミュニケーションの度合いに左右されると考えられ、被抑止国の行動によっては逆に不安定化を招きかねないことに留意する必要がある。

以上を総合すると、新領域と核兵器システムの関わりは核抑止を不安定化させる可能性が高いと言わざるを得ない。これに鑑みて、その安定化を図るうえでの政策課題は何かを考えてみたい。

まず、新領域をめぐる抑止について、関係国の間で認識の共有を図る必要がある。特に、新領域でのいかなる活動が許容されるのか、あるいは許容されないのかについての関係国相互の理解を形成していく努力が重要になる。ただし、こうした相互理解の形成がまだ十分でないうちは、例えばサイバー領域においてある国々が著しく破壊的な攻撃の実行を正当化しようとする潜在的可能性がある。また、許容し得るサイバー攻撃とは具体的にいかなる種類のものなのかに関する関係国の理解が曖昧で不明確になりがちであるために、意図しない偶発的なエスカレーションが起こり得る。さらに、新領域での関係国相互の競争的な活動が長く続いた結果、相対的なパワーシフトが生じて力関係が不安定化し、武力紛争に至る可能性もある[105]。このため、米国防大学のマンツォは、新領域において比例性を担保し得る攻撃は何か、またどのような攻撃がエスカレーションを招きやすいのかを判断するための共通の枠組みを潜在的敵対国との間で共有すべきだと主張する[106]。

他方で、比例性を欠いた報復の可能性を最初から排除しないことも重要であろう。新領域での攻撃に対して比例原則に基づく報復あるいはその脅しを発動したとしても、抑止効果は限定的と考えられ、攻撃を抑止できなかった場合にエスカレーションを防止することが難しくなるからである。例えば、電子攻撃を受けて衛星の機能が一時的に妨害されるような事態の場合は、攻撃元を特定した後に、報復として攻撃国の衛星に電子攻撃を発動するといった比例的な対応でもその後のエスカレーションを防止できる可能性はあるかもしれない。しかし、相手は比例原則に基づく報復しか行わないであろうと攻

撃国が判断した場合、新領域における抑止は困難となる。このため、比例性を欠いた報復の可能性を留保しておくことが抑止政策上は望ましいであろう。この際、どのような条件下であれば比例性を欠いた報復の信憑性を高め得るかを考えるべきである。また、国際人道法の比例原則との関係をどのように整理できるのかも課題となる。

さらに、領域横断的抑止の観点から、ある領域における核兵器システムへの攻撃をさせないために別の領域において核兵器によらない脅しを用いることができれば望ましい。一例として、NC3の宇宙アセットへの攻撃を抑止するために認知領域において脅しを用いることを検討してみたい。一般に、米国などの民主主義国に敵対的な権威主義国家は、国内のマスメディアを通じて政府が作成した政治的ナラティブを発信する一方で、そのナラティブと矛盾する事実が国内に広く配信されるのを防止しようとするであろう。この点を利用して、これらの権威主義国家が米国のNC3の宇宙アセットを攻撃しようとするのであれば、彼らの政治的ナラティブと矛盾する事実を報道する24時間テレビニュース番組を衛星放送により国民に向けて直接配信し、国民の支持を揺るがすことで権威主義体制の存続を困難にすると脅しをかけることは攻撃を抑止するうえで有効かもしれない[107]。ただし、こうした脅しの活用が民主主義の規範に則って適切なのかどうかを慎重に判断すべきと思われる。

新領域での脅威の出現状況を継続的に把握し、NC3への脅威を早期に発見し得る体制を整えることも重要な政策課題である。すでに米軍は宇宙・サイバー領域の監視体制を整え、宇宙状況把握やサイバー領域の監視活動などを継続的に行っている。しかし、NC3へのすべての脅威を把握できるわけではない。宇宙状況把握については、宇宙デブリなどの宇宙物体を監視し、これらが衛星に衝突するのを回避するための能力は向上しており、衛星に対する物理的な攻撃を把握することもある程度可能と思われるが、非物理的な攻撃の把握は難しいであろう。サイバー領域についても、サイバー攻撃に対する鑑識技術が発達してきてはいるものの、サイバー攻撃の技術も常に進化していることから鑑識にも限界がある[108]。これらの問題を克服するには大きなコストがかかると予想されるが、新領域におけるNC3へのさまざまな脅威を早期に発見し、核抑止の不安定化を防ぐためには必要な投資と考えるべきであろう。

核抑止の不安定化への対策として、NC3のレジリエンス向上を図っていかなければならない。米国は、NC3の近代化を進めるにあたって、特にEMPとサイバー脅威に対するレジリエンスを高める必要性を認識している[109]。米国のNC3は、①攻撃の探知・警告・特定、②核計画作成、③意思決定のための会議、④大統領命令の受領、⑤核部隊の管理と運用、の機能を果たすとされている[110]。このうち①については現行の早期警戒システムである「宇宙配備赤外線システム（Space-Based Infrared System: SBIRS）」を近代化するための「次世代OPIR（Overhead Persistent Infrared）」計画が進行中である[111]。②についても、現行の「統合戦略計画分析ネットワーク（Integrated Strategic Planning and Analysis Network: ISPAN）」のソフトウェアをアップデートする計画が進んでいる[112]。また、NC3の地上指揮センターが破壊された場合に空中から指揮を行うためのE-4B国家空中作戦センター（National Airborne Operations Center: NAOC）を近代化するにあたって、E-4Bの対EMP性の強化（EMP hardening）が検討されている[113]。サイバー対策については、次世代OPIR衛星開発の契約を請け負っているノースロップ・グラマンによれば、サイバー攻撃にも耐えられるシステム作りに取り組んでいるとされる[114]。米国のNC3近代化計画の全体像は明らかになっていないが、NC3のレジリエンス向上については引き続き関心を持って注視していく必要がある。

（2）新領域をめぐる拡大核抑止と「核の傘」国の役割

前項で、新領域が核抑止を不安定化させるのであれば、その安定化を図るうえでの政策課題は何かを考察した。この考察は核保有国の直接抑止、つまり自国に対する攻撃の抑止を前提としたものであったが、本項では核保有国の同盟国に対する拡大抑止の場合について検討してみたい。

具体的には、米国の拡大核抑止の供与を受ける「核の傘」国に焦点を置き、新領域・新興技術が「核の傘」国に対する米国の拡大核抑止を不安定化させる場合、その安定化を図るうえで「核の傘」国はいかなる役割を果たすべきなのかを考察する。

宇宙・サイバー・電磁波領域における攻撃は、必ずしも米国に対して行われるとは限らず、「核の傘」国に指向されることも考えられる。この場合、米国は自国が攻撃を受けていないにもかかわらず、攻撃国に何らかの報復をすべきか否かの判断を迫られるであろう。ヘリテージ財団のチェンは、米国の同盟国の宇宙アセットがジャミングなどの非物理的攻撃を受けた時、同盟国への攻撃に対する報復措置として米国は攻撃国の宇宙アセットにジャミング攻撃をすべきなのか、あるいは同盟国の指揮統制ネットワークがサイバー攻撃を受けた場合に、攻撃国に対して米国が行い得る比例的な報復とはどのようなものなのか、と問題提起している[115]。「核の傘」国に指向されたこれらの攻撃に対して米国が報復を含めた適切な対応を行わなかった場合は、米国のコミットメントに対する「核の傘」国の信頼感は低下し、拡大核抑止の不安定化を招くことが想定される。

こうした事態を防ぐために、「核の傘」国が果たすべき役割は何か。ここでは米韓同盟を例として、「核の傘」国である韓国が北朝鮮のサイバー攻撃を受けた場合について考えてみたい。米韓同盟として抑止・対処すべきサイバー攻撃は、その攻撃が戦略レベルの影響をもたらす重大なものと考えられ、例えば韓国の重要インフラや軍の指揮統制ネットワークを標的とした攻撃がこれに該当するであろう。米空軍のプラットは、①2009年7月の韓国政府機関などのウェブサイトに対する大規模DDoS攻撃、②2011年4月の韓国金融システムへのサイバー攻撃、③2013年3月および6月の韓国メディア・銀行・大統領府などへのサイバー攻撃、④2014年12月の韓国原発へのハッキングによる原発図面などのデータの流出、⑤2016年9月の韓国国防ネットワークへのサイバー攻撃による米韓機密情報の流出の5事案をリストアップし、このうち④と⑤を同盟として抑止すべき重大なサイバー攻撃としている。④と⑤の事案は、実際には戦略レベルの重大な影響を米韓両国にもたらしたわけではなかったが、将来的に同様の事案が起こる場合には重大な結果を招く恐れがあると予想されるからである。そのうえで、それ以外のサイバー攻撃には韓国が独力で対処することが望ましいと示唆している[116]。①から⑤までのすべての事案を同盟として抑止・対処するのは困難であるため、同盟が抑止すべき事案を戦略レベルのサイバー攻撃とし、それ以下のレベルの攻撃には韓国が対処することにより、サイバー攻撃をめぐる同盟としての抑止の焦点と韓国の果たすべき役割を明確にし得ると考えられる。ただし、戦略レベルの重大な影響をもたらすサイバー攻撃とそれ以下のレベルのサイバー攻撃を区別するのは現実には困難であり、その影響の程度は抑止が失敗した後に攻撃を受けて判定できるものであることから、前もって判断しておくことの妥当性は検討すべきであろう。

認知領域における攻撃が同盟分断政策の一環として「核の傘」国に指向される場合も考えられる。例えば、中国やロシアが偽情報による影響力工作を「核の傘」国に仕掛け、これらの国々の間に米国の拡大抑止コミットメントの継続性に対する疑念を生ぜしめようとするかもしれない。これが奏功した場合、共同の抑止行動に関する米国との調整を困難にするとともに、同盟として必要な核・非核および非キネティック能力をどのように組み合わせていくのかをめぐる米国との不協和音を助長するといったシナリオが検討されている[117]。こうしたシナリオが現実化するのを防止するために、「核の傘」国としては影響力工作に対する国民のレジリエンスを高めておく必要がある。北大西洋条約機構（North Atlantic Treaty Organization: NATO）においては、ソーシャルメディアを活用した認知戦が「核の傘」国を含むNATO加盟国の国民をターゲットとして展開される可能性が指摘されている。これに対抗するために、認知戦についての加盟国の認識を深めるとともに、民主主義国の開放性を逆手にとって市民社会を分断しようとする活動に対する加盟国国民のレジリエンスを向上させることの重要性が論じられている[118]。こうした認知戦が、米国の拡大抑止政策やNC3による意思決定プロセスへの「核の傘」国の信頼を動揺させる目的を持って展開される可能性もあるため、これに対する「核の傘」国のレジリエンス向上は核抑止の不安定化を防止するうえでの重要な役割といえる。

新興技術が核抑止を不安定化させる可能性について、米国と認識を共有しておくことも「核の傘」国の重要な役割であろう。例えば、AIをNC3の意思決定支援に活用した場合、NC3による意思決定プロセスはどうなるのか、核

抑止を不安定化させることはないのかなどの点について米国と協議し、認識を一致させておくことができれば望ましい。また、NC3ではなく、非核作戦を支援するシステムにAIが導入され、そのシステムとNC3が連接された場合の核抑止上の課題についても協議しておく必要があろう。現在、米国は軍のすべてのセンサーとシューターをリアルタイムで接続して戦う能力を目指す「統合全ドメイン指揮統制（Joint All Domain Command and Control: JADC2）」構想を推進中である。現時点では、JADC2は特定のネットワークやシステムを指すものではなく、米軍の新たな指揮統制のアプローチに関する取り組みとされている[119]。他方で、将来的にJADC2構想が何らかのシステムに収斂していくとすれば、JADC2システムは米軍の非核戦力を指揮統制するものとなろう。JADC2システムにはAIが導入される可能性があり、さらにそのシステムがNC3と連接されることも否定できないという[120]。その可能性はともかくとしても、JADC2はその名称が示すように新領域を含めた米軍の作戦能力向上を目指すものと理解され、それにAIが導入されていくとすれば、核抑止にも影響が及ぶものと考えられる。先述したように、そもそも非核作戦用のC3システムはNC3と両用となっていることから、JADC2システムへのAI導入はNC3にも影響を及ぼし得るものと理解すべきであろう。この点も踏まえつつ、「核の傘」国は新領域をめぐる拡大核抑止のありようについて米国と協議を深めていくべきと考える。

「核の傘」国の立場から、新領域・新興技術をめぐる拡大核抑止のアジェンダを提起し、同盟の核政策に反映させることができれば望ましい。NATOの核共有政策の場合、「核の傘」国が参加する枠組みには加盟国の一部による核兵器共有と、加盟国のほぼすべてが参加するNATO核計画グループ（Nuclear Planning Group: NPG）による核協議の2つがあり、「核の傘」国としてはそれぞれの政策枠組みにおいて課題を提起することとなろう。

NATOの核兵器共有は、NATOに加盟する「核の傘」国のうち5カ国（ベルギー、ドイツ、イタリア、オランダ、トルコ）に米国が戦術核爆弾B61を事前に配備しておき、有事の際に米国が大統領の許可の下でB61を5カ国に供与するとともに、5カ国は通常兵器・核兵器両用航空機（dual-capable aircraft: DCA）にB61を搭載して使用することを想定した枠組みである[121]。ブリュッセル自由大学のマットレアは、NATOの核兵器共有政策を領域横断的抑止の視点から再検討し、今日の安全保障環境の変化に迅速に適応できるようにしていくべきであり、そのためにもDCAのF-35ステルス戦闘機への換装やB61の近代化を進めていくのが望ましいと述べている[122]。B61の近代化については、命中精度を高めたB61-12の欧州への配備計画が進められており、DCAのF-35への換装と併せてNATOの局地的抑止力を強化するものと期待されている[123]。なお、2023年10月に米国防総省がB61シリーズの最新型となるB61-13を新たに開発すると発表しているが[124]、B61-13が戦闘機にも搭載可能な爆弾として開発されるのか、またDCA搭載用核爆弾として欧州に配備されるのかは現時点では不明である[125]。

こうした核戦力の近代化と並行して、新領域をめぐるNATOの拡大核抑止と核共有政策の在り方について、NATOの「核の傘」国がNPGなどにおいて課題を提起することにより、拡大核抑止を不安定化させないための政策的処方箋を議論していくことが望まれる。

インド太平洋地域においては、NATOの核兵器共有のような枠組みは存在しないものの、米国との2国間同盟における核協議の中で「核の傘」国が新領域をめぐる拡大核抑止のアジェンダを提起することは可能であろう。この際、政府間協議に加えて、政府関係者と民間有識者によるトラック1.5協議を活用し、「核の傘」国としてインド太平洋地域における新領域の脅威と拡大抑止の課題を提起することも有意義である[126]。

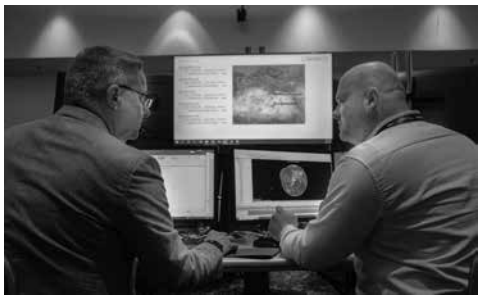
（3）軍備管理への期待と展望

近年、新領域に係る軍備管理の必要性を訴える有識者の声が高まっている。米セキュアワールド財団のサムソンらは、米国が主導して宇宙の安全および安定を強化するための宇宙軍備管理を含む法的拘束力のある措置を提案すべきだと述べている[127]。また、アメリカ・カトリック大学のモリーニは、サイバー領域での攻撃の応酬が国家間の緊張をエスカレートさせ、特に核保有国間でそれが起こった場合は重大な結果を招くことが懸念されることから、国際社

会はサイバー攻撃手段を規制するための努力を最優先すべきだと主張している[128]。これまで論じてきたように、新領域と核兵器システムの関わりが核抑止の不安定化を招く恐れがあることから、核保有国間の関係の安定を図るための軍備管理上の措置が求められてこよう。

ここでは、新領域と核兵器システムをめぐる軍備管理のアジェンダを考察していくこととし、まず宇宙領域における軍備管理について考えてみたい。

これまで考察したように、対衛星攻撃能力がNC3の宇宙アセットに対する脅威となっていることから、核抑止の不安定化を防止する観点からは、当該能力の規制が宇宙領域における軍備管理上の焦点と考えられる。これに関して、中国とロシアは法的拘束力を持つ軍備管理条約を目指す姿勢を堅持しており、2008年には宇宙空間における兵器配置防止条約（Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects: PPWT）案を共同で提出している。この条約案は、検証が困難であること、地上配備の対衛星攻撃兵器が含まれていないことなどの理由から交渉開始には至っていない。こうした中露の条約ベースのアプローチに対して、米国など西側諸国は宇宙の安全保障に対する最大の脅威は特定の兵器などではなく軌道上における行動（behavior and actions）であると考えており、宇宙における責任ある行動の規範を目指すアプローチを採っている[129]。西側諸国がこうした行動規範アプローチを追求する背景には、宇宙における「兵器」とは何かを定義することが難しいため、中露が追求するような特定の兵器の規制・管理を目指した従来の軍備管理のアプローチでは実効性に欠け、検証が事実上不可能になるとの認識がある。例えば、軌道上の衛星に接近して燃料補給や修理を行うための「ランデブー・近接オペレーション（rendezvous and proximity operation: RPO）」と呼ばれる活動は、標的となる衛星に正確に接近してこれを破壊する能力として使うことも可能である[130]。そうかといって、RPOを実施可能な宇宙アセットを「兵器」として規制しても無意味であるばかりか、衛星の保守に必要な活動に支障をきたすことになりかねない。他方で、行動規範アプローチにも限界がある。衛星へのジャミングは意図しない電波干渉により発生するノイズと区別することが難しく、対衛星サイバー攻撃は攻撃元の特定が困難であり、衛星へのレーザー攻撃の発信源を追跡して突き止めることも簡単ではない。このため、攻撃者は自己の行動を否定することが可能であり[131]、検証の可能性や透明性の確保が困難になる。



対衛星兵器模擬演習の様子（John Ayre／U.S. Space／Planet Pix via ZUMA Press Wire／共同通信イメージズ）

こうした限界はあるものの、行動規範アプローチにより、対衛星攻撃能力によるNC3の宇宙アセットへの脅威をある程度低減することはできるかもしれない。特に、NC3の宇宙アセットに対する攻撃を行わないことを国際的に合意するのは不可能ではなかろう。最初から国際協定の締結を目指すことが難しいようであれば、まずは攻撃の一方的な自制から始め、次いで非公式の合意を模索するというように段階を踏んで国際的な合意を形成していくことが望ましい[132]。宇宙領域の軍備管理をめぐっては、2020年12月に国連総会で「責任ある行動の規範、規則および原則を通じた宇宙における脅威の低減（Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviours）」決議が採択され、同決議に基づく国連作業部会の初会合が2022年5月にジュネーブで開催されている[133]。こうした国際社会の努力が、NC3の宇宙アセットに対する攻撃を行わないことへの合意に結実し、核抑止の不安定化を防止することにつながることが期待される。

次に、サイバー領域における軍備管理を検討する。宇宙領域と同様に、サイバー領域においても「兵器」とは何かを定義することは困難であり、従来の軍備管理アプローチでは実効性や透明性を確保できない恐れがある。レスター大学のフッターは、いわゆる「サイバー兵器」が普通の兵器と異なり実体のない存在であるため、軍備管理の対象とするのは難しいことから、サイバー領域の規制にあたってはサイバー攻撃の標的（targets）あるいは行動（actions）を規制の対象とするのが有意義なのではないかと示唆している[134]。この見方を

踏まえれば、実体のない「サイバー兵器」を全般的に禁止あるいは規制するのではなく、例えばNC3を標的としたサイバー攻撃という行動を規制の対象とするといったように、核抑止を不安定化させる要素に限定して規制をかけることが軍備管理上意味のある方策だと言うことができよう。具体的な措置の一案として、戦略国際問題研究所のウィリアムズらは、ウクライナ戦争後に米中露が相互のNC3に対するサイバー攻撃を自制する旨の非公式な合意を交わすオプションも考えられると述べている[135]。

電磁波領域における軍備管理については、先述したアンダーソンらの指摘にあるように、指向性エネルギー兵器が戦域以下のレベルの核兵器システムを無力化し得る潜在的可能性があることに鑑みて、これらの核兵器システムに対する指向性エネルギー兵器の使用を規制する枠組みを検討することが望ましい。特に、NATO加盟5カ国への配備が進められている米国のB61-12戦術核爆弾には命中精度を高めるための慣性誘導装置が搭載されており[136]、指向性エネルギー兵器の影響を受ける恐れがあるとすれば、こうした枠組みはNATOの核抑止の安定化に寄与すると思われる。ただし、指向性エネルギー兵器そのものに規制をかける従来の軍備管理のアプローチではなく、核抑止を不安定化させる恐れのある指向性エネルギー兵器の使用という「行動」を規制の対象とし、核抑止の安定化のうえで避けるべき行動を示す規範的アプローチを追求することが望ましいであろう。こうしたアプローチは、次の認知領域における問題にも通じるものである。

認知領域における軍備管理のアジェンダには、電磁波領域と重なる部分もあるが、人間の脳を標的とした指向性エネルギー兵器による攻撃の規制を含むことも検討していく必要があろう。先述したように、電磁波を用いて人間の脳を直接攻撃する兵器の開発が始まっているとされており、こうした兵器や攻撃方法がより高度化していけば核兵器システムに関わる要員を標的とした攻撃も可能になるかもしれない。仮に核使用の意思決定者が攻撃を受けた場合、判断や決心に悪影響が生じて核抑止が不安定化する恐れは否定できない。このように、「ニューロストライク」兵器は危機における先制攻撃の誘因を生ぜしめ、戦争のリスクを高める潜在的可能性があるとして、これらの兵器を規制するための軍備管理努力が早急に求められると指摘されている[137]。

新興技術をNC3に導入した場合の核抑止上のリスクに鑑みて、これを規制するための軍備管理の必要性も指摘されている。特にAIについては、外交問題評議会のカーンは核保有国が自信を持ってNC3に組み込めるだけの技術的成熟度にAIはまだ至っていないとして、核抑止を不安定化させて核使用の可能性を高める恐れのあるAIの活用を規制するよう核保有国間で早期に合意すべきだと主張する[138]。ここでも、AIを「兵器」として規制をかける従来の軍備管理のアプローチではなく、核抑止を不安定化させる恐れのあるAIの使用という「行動」を避けるべきとする規範的アプローチが将来に向けた重要な一歩になると思われる。これに関連して、AIが実装された核兵器システムに対してサイバー攻撃を行い、AIの訓練データを書き換えて相手の核兵器システムを無力化させる可能性も指摘されている[139]。こうした可能性を想定しつつ、核兵器システムに実装されたAIを標的とするサイバー攻撃という特定の「行動」も避けるべき対象とするかどうかも検討すべきである。

これに対して、極超音速兵器の規制については従来の軍備管理のアプローチを適用できる余地がある。カリフォルニア大学グローバル紛争・協力研究所のウォーレンは、ロシアとの戦略核兵器削減交渉を有利に進めるとともに、中距離核戦力の上限を再確立するための手段として、米国が極超音速兵器の制限をロシアに持ち掛けることにより米露間の核軍備管理協定への道筋をつけ、ゆくゆくはこれに中国を引き込んでいくことができれば望ましいとしている[140]。ただし、こうした交渉に際して、中露が米国のミサイル防衛システムを規制の対象に含めるように求めてくる可能性が高いことに留意する必要があろう。もともと中露が極超音速兵器の開発を始めた背景には、中露に対する米国のミサイル防衛能力の優位性に直面した両国が、ミサイル防衛システムを回避して報復攻撃を遂行できる第二撃能力の確保を目指したことがあり、その意味で米国のミサイル防衛の規制は中露両国にとって極超音速兵器の規制と引き換えにしても利益の方が大きいと判断されるかもしれない。このため、今後の米露（中）軍備管理のアジェンダに極超音速兵器の規制が含まれるとすれば、米国のミサイル防衛の規制とセットで議論されるようになると思われる。

なお、新興技術の規制については、すでに確立された兵器技術を規制するよりも合意形成が容易かもしれないとの見方もある[141]。実際に、ロシアが2020年に米露間の新戦略兵器削減条約（New Strategic Arms Reduction Treaty: New START、以下、新START）の期限延長と引き換えに、開発したばかりの極超音速滑空兵器「アヴァンガルド」を新型ICBM「サルマト」とともに新STARTの規制対象に含める用意があると提案した事例がある[142]。

新興技術を規制するばかりでなく、軍備管理に裨益するように活用することも考える価値があろう。AIを軍備管理における検証に活用する可能性について先述したが、量子技術を活用して核兵器を監視し、軍備管理協定の履行状況の検証を強化し得る可能性もある。前出のヘイズは、中立的で公平な早期警戒融合センター（an independent, impartial early warning fusion center）を設立し、量子技術を活用して得られた監視・検証データに基づいて核保有国に適切な助言を行うことができれば軍備管理上望ましいとしている[143]。

おわりに

本章では、新領域、つまり宇宙・サイバー・電磁波・認知の各領域における活動が核兵器システムにどのように関わり、いかなる影響を及ぼすのかを考察した。その中で、新領域と核兵器システムとの関わりが核抑止を安定化させるのか、それとも不安定化させるのかを問いとして設定した。なお新興技術については、AIがサイバー攻撃能力の強化に寄与するといったように、新領域での活動のイネーブラーとして作用するという側面があり、新領域の動向に少なからぬ影響を及ぼすものとして分析を行った。新領域と核兵器システムとの関わりが核抑止を安定化させる可能性について、宇宙・サイバー領域における攻撃の相互自制、認知領域の活用による核使用の抑止、新興技術の導入による核使用の抑制を検討した。ただし、それぞれの可能性は新領域をめぐる被抑止国との関係あるいはコミュニケーションの度合いに左右されるとして、被抑止国の行動によっては逆に不安定化を招きかねないことを指摘した。また、核抑止の不安定化を招く恐れとしては、新領域による第二撃能力の脆弱化、新領域での攻撃に対する報復的抑止の実効性の問題、意図せざる核兵器使用の可能性の高まりを挙げた。総じて、新領域と核兵器システムの関わりは核抑止を不安定化させる可能性が高いと結論付けた。

これに鑑みて、本章では①新領域による核抑止の不安定化への政策課題、②新領域をめぐる拡大核抑止と「核の傘」国の役割、③軍備管理への期待と展望について論述した。①については米国の直接抑止を念頭に置き、新領域をめぐる抑止についての関係国間での認識の共有、比例性を欠いた報復の可能性の留保、領域横断的抑止の脅しの活用、新領域に対する監視体制の整備、NC3のレジリエンス向上を政策課題とした。②については、同盟として抑止すべき戦略レベルの攻撃とそれ以下のレベルの攻撃を区別し、「核の傘」国は後者に独力で対処すること、認知領域での攻撃に対する「核の傘」国のレジリエンス向上を図っていくこと、「核の傘」国として新領域・新興技術をめぐる拡大核抑止についての課題を提起していくことを挙げた。最後に、③については宇宙・サイバー・電磁波・認知の各領域における軍備管理を検討するとともに、新興技術の規制と軍備管理への活用を検討した。特に、新領域における軍備管理を追求するにあたっては、特定の兵器の規制・管理を目指す従来の軍備管理のアプローチでは実効性に欠け、検証が事実上不可能になることから、核抑止を不安定化させる恐れのある新領域での「行動」を規制の対象とし、核抑止の安定化のうえで避けるべき行動を示す規範的アプローチを追求することが将来に向けた重要な一歩になるとした。

本章で考察した新領域と核兵器システムの関わりについては、考え得るあらゆる事態を網羅的に検討したものではなく、現時点で有識者の間で議論されているいくつかの事態や問題認識などに基づいて分析を試みたものに過ぎない。それにもかかわらず、現時点で注目されている宇宙・サイバー・電磁波・認知の各領域が新興技術の急速な発展に伴って遠からず進化を遂げ、核兵器システムにさらなる負荷をかけ、核抑止の不安定化を促進していくかのような近未来を想像することは可能であろう。もちろん核兵器システムの側も近代化を進めて新領域の脅威に対抗しようとするであろうが、少なくともサイバーセキュリティに限っては旧式のアナログシステムの方が近代的なデジタルシ

ステムよりもサイバー攻撃の影響を受けにくかったとされているように[144]、核兵器システムの近代化はけっして万能ではない。こうした近未来図は、今後さらに新たな領域が出現して核抑止に未知の影響を及ぼしてくる事態をも予期させるものである。その意味で、本章で考察した新領域と核兵器システムをめぐる問題群から、「核時代の新たな地平」の一局面が多少なりとも垣間見えてくることを期待したい。

1) King Mallory, "New Challenges in Cross-Domain Deterrence," *Perspective*, RAND Corporation (2018), 1.
2) 領域横断的抑止（cross-domain deterrence: CDD）という用語は2000年代後期に米国の国防当局者の間で使用され始めたという。Eric Gartzke and Jon R. Lindsay, eds., *Cross-Domain Deterrence*: *Strategy in an Era of Complexity* (New York: Oxford University Press, 2019), 4.
3) Tim Sweijs and Samo Zilincik, "Cross-Domain Deterrence and Hybrid Conflict," Hague Centre for Strategic Studies (December 2019), 11-12. なお、「複合的抑止」概念については次を参照。T. V. Paul, Patrick M. Morgan, and James J. Wirtz, eds., *Complex Deterrence*: *Strategy in the Global Age* (Chicago: University of Chicago Press, 2009).
4) これを含め、以降の本章における人物の所属および肩書はいずれも当時のものである。
5) Gartzke and Lindsay, *Cross-Domain Deterrence*, 6.
6) Sweijs and Zilincik, "Cross-Domain Deterrence and Hybrid Conflict," 15-16.
7) Jacek Durkalec, Paige Gasser, and Oleksandr Shykov, "Multi-Domain Strategic Competition: Rewards and Risks," Workshop Summary, Center for Global Security Research, Lawrence Livermore National Laboratory (November 2018), 11-12.
8) Vincent Boulanin et al., "Artificial Intelligence, Strategic Stability and Nuclear Risk," Stockholm International Peace Research Institute (June 2020), 105.
9) 戸崎洋史「新興技術と核抑止関係」日本国際問題研究所、2021年3月30日。
10) Marie Villarreal Dean, "U.S. Space-Based Nuclear Command and Control: A Guide," Center for Strategic and International Studies (January 2023), 1-5.
11) Don Snyder and Alexis A. Blanc, "Unraveling Entanglement: Policy Implications of Using Non-Dedicated Systems for Nuclear Command and Control," RAND Corporation (2023), 1-8.
12) Stephen M. McCall, "Space as a Warfighting Domain: Issues for Congress," *CRS in Focus*, no. IF 11895, Congressional Research Service (August 10, 2021).
13) Kari A. Bingen, Kaitlyn Johnson, and Makena Young, "Space Threat Assessment 2023," Center for Strategic and International Studies (April 2023), 4.
14) Ibid., 11-14.
15) Ed Browne, "Fact Check: Did Russia Use Lasers to Target Satellites over Ukraine Border?" *Newsweek*, October 5, 2022.
16) Bruce Blair, "Why Our Nuclear Weapons Can Be Hacked," *New York Times*, March 14, 2017.
17) Garrett K. Hogan, "The Electromagnetic Spectrum: The Cross Domain," Joint Air Power Competence Centre (November 2015).
18) Elżbieta Hodyr, "Cybersecurity of Nuclear Weapon Systems," *Cybersecurity and*

Law 6, no. 2 (2021): 94-95.
19) Natasha Bertrand and Eric Wolff, "Nuclear Weapon Agency Breached amid Massive Cyber Onslaught," *Politico*, December 17, 2020.
20) "Russian Hackers Targeted US Nuclear Research Laboratories, Records Reveal," *Guardian*, January 6, 2023.
21) Bishr Tabbaa, "Zer0 Days: How Stuxnet Disrupted the Iran Nuclear Program and Transformed Computer Security," *Medium*, July 17, 2020.
22) Kayla T. Matteucci, "Protecting Nuclear Command, Control, and Communications below the Threshold of Armed Conflict: Don't Count on Deterrence," Institute for Defense Analyses (June 2021), 31.
23) Juliana Suess, "Jamming and Cyber Attacks: How Space Is Being Targeted in Ukraine," RUSI, April 5, 2022.
24) Ariel Cohen, "Protecting America's Power Grids from EMP Attacks," *Forbes*, May 20, 2023.
25) Oriana Pawlyk, "Air Force Wants to Harden the B-2 Bomber to Withstand an EMP Attack," Military.com website.
26) "HiJENKS Missile: Bold Innovation from US Navy and Air Force Labs," SOFREP, July 7, 2022.
27) Peter Pry, "Non-Nuclear Electromagnetic Pulse (NNEMP) Attack on the U.S. Power Grid," Worldview Weekend Broadcast Network, June 21, 2021.
28) Theresa Hitchens, "Laser Weapons 'Finally' Seeing 'Real Progress,' Missile Defense Agency Official Says," *Breaking Defense*, August 17, 2023.
29) Justin Anderson and James R. McCue, "Deterring, Countering, and Defeating Conventional-Nuclear Integration," *Strategic Studies Quarterly* 15, no. 1 (Spring 2021): 48.
30) Mana Alahmad, "Strengths and Weaknesses of Cognitive Theory," *Budapest International Research and Critics Institute-Journal (BIRCI-Journal) Humanity and Social Sciences* 3, no. 3 (July 2020): 1584.
31) Bernard Claverie and François Du Cluzel, "'Cognitive Warfare': The Advent of the Concept of 'Cognitics' in the Field of Warfare," in *Cognitive Warfare*: *The Future of Cognitive Dominance*, Bernard Claverie et al., NATO Collaboration Support Office (2022), 2, 1-7.
32) Jean-Marc Rickli, Federico Mantellassi, and Gwyn Glasser, "Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century," Policy Brief, Geneva Centre for Security Policy, August 25, 2023.
33) United States Senate Select Committee on Intelligence, "Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election," vol. 1, 1-5.
34) Robert McCreight, "Neuro-Cognitive Warfare: Inflicting Strategic Impact via Non-Kinetic Threat," *Small Wars Journal*, September 16, 2022.
35) Sam Meyer, "Fake News, Real Consequences: The Dangers of WMD Disinformation," NTI, December 7, 2017.
36) Heather Williams and Alexi Drew, "Escalation by Tweet: Managing the New Nuclear Diplomacy," King's College London, July 2020.
37) Matty S. Golub, "Who's to Say?: Technical Dimensions of Nuclear Disinformation," *On the Horizon*: *A Collection of Papers from the Next Generation* (February 2021), 72-82.
38) Rebecca Hersman, "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review* 3, no. 3 (Autumn 2020): 96-97.
39) Marcy Fowler, Elin Bergner, and Kristiana Nitisa, "Combating Nuclear Misinformation and Disinformation: Tools, Approaches and the Role of NGOs and International Organizations," Open Nuclear Network (November 2022), 2.
40) Rajeswari Pillai Rajagopalan, "Introduction," in *Future Warfare and Technologies*: *Issues and Strategies*, Observer Research Foundation, November 24, 2022.
41) Adam Lowther, "The Big and Urgent Task of Revitalizing Nuclear Command, Control, and Communications," *War on the Rocks*, October 4, 2019.
42) Charles Beames, "AI in Space and Its Future Use in Warfare," *Forbes*, December 21, 2022.
43) James Johnson and Eleanor Krabill, "AI, Cyberspace, and Nuclear Weapons," *War on the Rocks*, January 31, 2020.
44) Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China" (2022), 161-162.
45) Travis Hallen and Michael Spencer, "Hypersonic Air Power," Air Power Development Centre, Royal Australian Air Force, June 25, 2018.
46) Roman C. Lau, "Hypersonic Impacts: Operational Impacts of Hypersonic Weapons and the Change of America's Strategic Situation," Joint Advanced Warfighting School, Joint Forces Staff College, National Defense University (May 2021), 46.
47) Demetri Sevastopulo and Kathrin Hille, "China Tests New Space Capability with Hypersonic Missile," *Financial Times*, October 16, 2021.
48) Jason Sherman, "Hypersonic Weapons Can't Hide from New Eyes in Space," *Scientific American*, January 18, 2022.
49) Senate Armed Services Committee, "Statement of Charles A. Richard, Commander, United States Strategic Command before the Senate Armed Services Committee," March 8, 2022, 25-26.

50) Peter Hayes, “Nuclear Command-and-Control in the Quantum Era,” Nautilus Institute, March 29, 2018.
51) Hamish Johnston, “Beijing and Vienna Have a Quantum Conversation,” *Physics World*, September 27, 2017.
52) Sarah Jacobs Gamberini and Lawrence Rubin, “Quantum Sensing’s Potential Impacts on Strategic Deterrence and Modern Warfare,” *Orbis* 65, no. 2 (Spring 2021): 360-362.
53) Durkalec, Gasser and Shykov, “Multi-Domain Strategic Competition,” 12.
54) Erica Lonergan and Keren Yarhi-Milo, “Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis,” *War on the Rocks*, April 21, 2022.
55) David C. Gompert and Phillip C. Saunders, “Sino-American Strategic Restraint in an Age of Vulnerability,” *Strategic Forum*, no. 273 (January 2012): 2-8.
56) Sitki Egeli, “Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability,” *Journal for Peace and Nuclear Disarmament* 4, no. 1 (2021): 124-125.
57) Patrick Morgan, *Deterrence*: *A Conceptual Analysis* (Beverly Hills, CA: Sage Publication, 1977), 31-43.
58) James Johnson, “Escalation to Nuclear War in the Digital Age: Risk of Inadvertent Escalation in the Emerging Ecosystem,” Modern War Institute, October 13, 2021.
59) Paul A. Goossen, “Cognitive Targeting: A Coercive Air Power Theory for Conventional Escalation Control against Nuclear-Armed Adversaries,” School of Advanced Air and Space Studies, Air University (June 2016), 61-96.
60) Edward Geist and Andrew J. Lohn, “How Might Artificial Intelligence Affect the Risk of Nuclear War?” RAND Corporation (2018), 21.
61) Jessica Cox and Heather Williams, “The Unavoidable Technology: How Artificial Intelligence Can Strengthen Nuclear Stability,” *Washington Quarterly* 44, no. 1 (2021): 73-77. 同様の見方として、次を参照。Jennifer Spindel, “Artificial Intelligence and Nuclear Weapons: Bringer of Hope or Harbinger of Doom?” *European Leadership Network*, August 17, 2020.
62) Tess Skyrme, “Quantum Sensors: Advancing Timing, Navigation, Mapping, & Brain Scans,” *IDTechEx*, August 2, 2023.
63) Katarzyna Kubiak, “Quantum Technology and Submarine Near-Invulnerability,” European Leadership Network (December 2020), 3-9.
64) Geist and Lohn, “How Might Artificial Intelligence Affect the Risk of Nuclear War?” 6.
65) Eva Nour Repussard, “Cyber-Nuclear Nexus: How Uncertainty Threatens Deterrence,” Project on Nuclear Issues, Center for Strategic and International Studies, May 10, 2023.
66) Barry Pavel and Christian Trotti, “New Tech Will Erode Nuclear Deterrence. The US Must Adapt,” *Defense One*, November 4, 2021.
67) Paul Bracken, “The Hunt for Mobile Missiles: Nuclear Weapons, AI, and the New Arms Race,” Foreign Policy Research Institute, September 21, 2020.
68) Dean Wilkening, “Hypersonic Weapons and Strategic Stability,” *Survival* 61, no. 5 (October-November 2019): 136-137.
69) Pavel Podvig, “The Myth of Strategic Stability,” Bulletin of the Atomic Scientists, October 31, 2012.
70) Matthew Kroenig, “Will Emerging Technology Cause Nuclear War?: Bringing Geopolitics Back In,” *Strategic Studies Quarterly* 15, no. 4 (Winter 2021): 59-62.
71) “Quantum Computing and Artificial Intelligence Expected to Revolutionize ISR,” Strategic Alternatives Branch, Strategic Plans and Policy, NATO, September 30, 2022.
72) James Johnson, “The AI-Cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability,” *Journal of Cyber Policy* 4, no. 3 (2019): 448.
73) Michael P. Gleason and Peter L. Hays, “Getting the Most Deterrent Value from U.S. Space Forces,” Center for Space Policy and Strategy (October 2020), 4-5.
74) Roger G. Harrison, Deron R. Jackson, and Collins G. Shackelford, “Space Deterrence: The Delicate Balance of Risk,” *Space and Defense* 3, no. 1 (Summer 2009): 11-14.
75) Sico van der Meer, “Deterrence of Cyber-Attacks in International Relations: Denial, Retaliation and Signaling,” *International Affairs Forum* (Spring 2017), 86.
76) Samantha Ravich and Mark Montgomery, “Harden the Cybersecurity of US Nuclear Complex Now,” *C4ISRNet*, October 26, 2022.
77) Kazuto Suzuki, “A Japanese Perspective on Space Deterrence and the Role of the Japan-US Alliance in Sino-US Escalation Management,” in *Outer Space*; *Earthly Escalation*? *Chinese Perspectives on Space Operations and Escalation*, ed. Nicholas Wright, Department of Defense (August 2018), 45.
78) Matthew R. Crook, “Nuclear Deterrence and the Space and Cyber Domains,” Naval Postgraduate School (October 2022), 25.
79) Tim Sweijs and Samuel Zilincik, “The Essence of Cross-Domain Deterrence,” in *Deterrence in the 21st Century*: *Insights from Theory and Practice*, ed. Frans Osinga and Tim Sweijs, Springer (2020), 134.
80) Timothy Georgetti, “U.S. Deterrence in Space: Confusing Constellations for Stars,” *Dauntless*, August 28, 2023.
81) Harrison, Jackson, and Shackelford, “Space Deterrence,” 22-25.
82) Matthias Schulze, “Cyber Deterrence is Overrated,” SWP Comment, no. 34 (August 2019), 3.

83) Crook, "Nuclear Deterrence and the Space and Cyber Domains," 23.
84) Scott D. Sagan and Allen S. Weiner, "The U.S. Says It Can Answer Cyberattacks with Nuclear Weapons. That's Lunacy," *Washington Post*, July 9, 2021.
85) Benjamin Bahney and Anna Péczeli, "The Role of Nuclear-Conventional Intermingling on State Decision-Making and the Risk of Inadvertent Escalation," NSI (November 2021), 7-8.
86) Ankit Panda, "Space-Based Nuclear Command and Control and the 'Non-Nuclear Strategic Attack,'" *Diplomat*, April 8, 2020.
87) James M. Acton, "Cyber Warfare & Inadvertent Escalation," *Daedalus* 149, no. 2 (Spring 2020): 137-141.
88) Chen Dongxiao, "Forewords," in *China-U.S. Cyber-Nuclear C3 Stability*, ed. Ariel E. Levite et al., Carnegie Endowment for International Peace (April 2021), iv.
89) Bill Gertz, "New Strategic Threat Emerging as Weapons Seek to Target Brain Function, Inflict Neurological Damage," *Washington Times*, May 24, 2023.
90) McCreight, "Neuro-Cognitive Warfare."
91) 戸崎「新興技術と核抑止関係」。
92) Geist and Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" 2-4.
93) Silky Kaur, "One Nuclear-Armed Poseidon Torpedo Could Decimate a Coastal City. Russia Wants 30 of Them," Bulletin of the Atomic Scientists, June 14, 2023.
94) Jill Hruby and M. Nina Miller, "Assessing and Managing the Benefits and Risks of Artificial Intelligence in Nuclear-Weapon Systems," NTI (August 2021), 12-25.
95) Amber Afreen Abid, "Artificial Intelligence in the Nuclear Age," Strategic Vision Institute, October 4, 2023.
96) Nicholas Thompson, "Inside the Apocalyptic Soviet Doomsday Machine," *Wired*, September 21, 2009.
97) Anthony M. Barrett, "False Alarms, True Dangers? Current and Future Risks of Inadvertent U.S.-Russian Nuclear War," RAND Corporation (2016), 11.
98) "Risks of Artificial Intelligence in Nuclear Command, Control and Communications (NC3): Primer & Policy Options for Risk Mitigation," Future of Life Institute (July 2023), 6-7.
99) Peter Rautenbach, "Keeping Humans in the Loop is not Enough to Make AI Safe for Nuclear Weapons," Bulletin of the Atomic Scientists, February 16, 2023.
100) Alice Saltini, "To Avoid Nuclear Instability, a Moratorium on Integrating AI into Nuclear Decision-Making Is Urgently Needed: The NPT PrepCom Can Serve as a Springboard," European Leadership Network, July 28, 2023.
101) Sweijs and Zilincik, "Cross-Domain Deterrence and Hybrid Conflict," 15.
102) Harrison, Jackson, and Shackelford, "Space Deterrence," 23-24.
103) Iain King, "What Do Cognitive Biases Mean for Deterrence?" *Strategy Bridge*, February 12, 2019.
104) Natasha E. Bajema and John Gower, "Nuclear Decision-Making and Risk Reduction in an Era of Technological Complexity," Council on Strategic Risks (December 2022), 96-97.
105) Michael P. Fischerkeller and Richard K. Harknett, "What Is Agreed Competition in Cyberspace?" *Lawfare*, February 19, 2019.
106) Vincent Manzo, "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit," *Strategic Forum*, no. 272 (December 2011): 3-7.
107) Mallory, "New Challenges in Cross-Domain Deterrence," 11.
108) 鈴木一人「安全保障の空間的変容」『国際問題』第 658 号（2017 年 1・2 月）10 頁。
109) Steven Aftergood, "USAF Seeks 'Resilient' Nuclear Command and Control," Federation of American Scientists, April 24, 2019.
110) Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, *Nuclear Matters Handbook 2020*, 21-22.
111) John R. Hoehn, "Nuclear Command, Control, and Communications (NC3) Modernization," *CRS In Focus*, no. IF11697, Congressional Research Service (December 8, 2020).
112) U.S. Air Force, "Battle Management Working to Improve Nuclear Scenario Planning," October 26, 2014.
113) Theresa Hitchens, "Air Force to Kick Off E-4B Replacement Competition in 2021," *Breaking Defense*, February 14, 2020.
114) Courtney Albon, "Northrop Missile-Warning Satellites Pass Early Design Review," *C4ISRNet*, May 24, 2023.
115) Dean Cheng, "Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC," Heritage Foundation, January 21, 2016.
116) James E. Platte, "Defending Forward on the Korean Peninsula: Cyber Deterrence in the U.S.-ROK Alliance," *Cyber Defense Review* 5, no. 1 (Spring 2020): 78-83.
117) Heather Williams et al., "Alternative Nuclear Futures: Capability and Credibility Challenges for U.S. Extended Nuclear Deterrence," Center for Strategic and International Studies (May 2023), 14.
118) Johns Hopkins University & Imperial College London, "Countering Cognitive Warfare: Awareness and Resilience," *NATO Review*, May 20, 2021.
119) 菊地茂雄「中国の軍事的脅威に関する認識変化と米軍作戦コンセプトの展開――統合全ドメイン指揮統制（JADC2）を中心に」『安全保障戦略研究』第 2 巻第 2 号（2022 年 3 月）42 頁。
120) Michael Klare, "The Military Dangers of AI Are Not Hallucinations," *Foreign Policy in Focus*, July 14, 2023.

121) David Cenciotti, "Let's Have a Look at This Year's NATO Nuclear Strike Exercise in Europe," *Aviationist*, October 28, 2022.
122) Alexander Mattelaer, "Rethinking Nuclear Deterrence: A European Perspective," Centre for Security, Diplomacy and Strategy (May 2022), 5-6.
123) Frank Kuhn, "Making Nuclear Sharing Credible Again: What the F-35A Means for NATO," *War on the Rocks*, September 14, 2023.
124) U.S. Department of Defense, "Department of Defense Announces Pursuit of B61 Gravity Bomb Variant," Immediate Release, October 27, 2023.
125) Aaron Mehta, "US to Introduce New Nuclear Gravity Bomb Design: B61-13," *Breaking Defense*, October 27, 2023.
126) Bates Gill, "Meeting China's Emerging Capabilities: Countering Advances in Cyber, Space, and Autonomous Systems," National Bureau of Asian Research, December 15, 2022.
127) Victoria Samson and Brian Weeden, "Enhancing Space Security: Time for Legally Binding Measures," Arms Control Association (December 2020).
128) Gabriel Molini, "The Evolving Cyber-Based Threat: The Need for International Regulations to Avoid 'Accidental' Conflicts," Center for Arms Control and Non-Proliferation, September 12, 2023.
129) Victoria Samson, "Breaking the Impasse over Security in Space," Arms Control Association (September 2022).
130) Mary Chesnut, "The 21st Century-Space Race Is Here," *National Interest*, October 17, 2019.
131) Ibid.
132) United Nations Institute for Disarmament Research, "Restoring Confidence across Today's Nuclear Divides: Symposium Report," UNIDIR (2021), 5.
133) Daryl G. Kimball, "Space Security Working Group Meets," Arms Control Association (June 2022).
134) Andrew Futter, "What Does Cyber Arms Control Look Like? Four Principles for Managing Cyber Risk," European Leadership Network (June 2020).
135) Heather M. Williams and Nicholas Smith Adamopoulos, "Arms Control after Ukraine: Integrated Arms Control and Deterring Two Peer Competitors," Center for Strategic and International Studies (December 2022), 8.
136) "B61-12 Nuclear Bomb," Airforce-technology.com website.
137) "Neuroweapons: Breakthroughs in Science Change Future Weapons," *Vision of Humanity*, n.d.
138) Lauren Kahn, "Mending the 'Broken Arrow': Confidence Building Measures at the AI-Nuclear Nexus," *War on the Rocks*, November 4, 2022.
139) Zachary Kallenborn, "AI Risks to Nuclear Deterrence Are Real," *War on the Rocks*, October 10, 2019.
140) Spenser A. Warren, "Avangard and Transatlantic Security," Center for Strategic and International Studies, September 23, 2020.
141) UNIDIR, "Restoring Confidence across Today's Nuclear Divides," 5.
142) "Russia Shows Willingness to Include New Nuke, Hypersonic Weapon in Arms Control Pact," *Defense News*, April 18, 2020.
143) Hayes, "Nuclear Command-and-Control in the Quantum Era."
144) Sandra Erwin, "Mattis to Decide Future of Nuclear Command, Control and Communications," *Space News*, April 11, 2018.