第1部
安全保障目的の宇宙利用を取り巻く環境の変化

第１章　センシングとセンスメイキングをめぐる競争での勝利

ブライアン・クラーク

1. はじめに：ポスト・ドミナンス期における同盟国の強みの活用

米軍は過去半世紀の間、潜在的及び実際の敵対者に対する広範な優勢を享受してきた。米軍は、強力な同盟ネットワークと世界で最も強固な防衛研究開発（R&D）基盤に支えられ、ネットワーク化された精密誘導打撃戦という当時としては新しいアプローチを適用することにより、「砂漠の嵐作戦」、及び「アライド・フォース作戦」で敵対者を打ち負かした。また、イラクとアフガニスタンにおける反乱に苛立ちはしたものの、そのような主に戦略的な失敗は、米軍の能力に不足があるためとは考えられていない。

米軍のドミナンス期は、予測されたとおり、今や終わりつつある。冷戦後期に米国国防総省が開発したセンサー、精密誘導兵器、ネットワーク、データ処理能力は広く普及し、ウクライナ、紅海、及びコーカサスにおいて、国家及び非国家集団により戦闘に使用されている[1]。それに加えて、精密誘導打撃戦の基盤技術（全地球測位システム、衛星通信、自律型ドローン）が商業化されたことにより、イエメンにおけるフーシー派反政府勢力のような敵対者が、国防総省における防衛費のごく一部に当たる費用で、米軍と同盟国軍を脅かすことが可能になっている。

米軍のドミナンスの衰えは、中華人民共和国（中国）との関係において最も顕著である。30年間に及ぶ近代化により、中国の人民解放軍（PLA）は国防総省の精密誘導打撃戦の構想を新たなレベルへ引き上げ、図1に示すように、あらゆるドメインに及ぶセンサーや、海、陸、空の何千もの誘導兵器発射装置から成る広

---

[1] Defense Intelligence Agency (DIA), *Iran: Enabling Houthi Attacks Across the Middle East*, (Washington, DC: DIA, 2024), https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Iran_Houthi_Final2.pdf; David Barno and Nora Bensahel, "Learning From Real Wars: Gaza And Ukraine," War on the Rocks, December 6, 2023, https://warontherocks.com/2023/12/learning-from-real-wars-gaza-and-ukraine/.

範なネットワークを展開している。

西太平洋における PLA と米国の軍事力の非対称性は、その大半が中国の戦略地政学上の優位によるものである。PLA は重要な相互防衛の責任を有しておらず、その近代化及び戦力態勢において、台湾や南シナ海の支配、及び米国や同盟国による介入の防止といった狭い範囲における主要な利益の追求に集中できる[2]。対照的に、米軍は、中国やロシアのような直接的な挑戦者である国家のみならず、イランや北朝鮮、及びその非国家代理勢力といった、主に米国の同盟国に対する脅威となる対戦相手にも対処することが期待されている。PLA の構造と組織は、中国の「近海」の防衛に重点を置いている。PLA の空軍（PLAAF）及び海軍（PLAN）は、複数の任務を行う軍隊を全世界に展開するのではなく、実質的な給油や兵站の能力を近代化の一部として配備しておらず、中国本土に拠点を置く PLA の防衛機能から離れて自衛と攻撃を行う能力を欠いたプラットフォームに

[2] Timothy Heath and Andrew S. Erickson, “Is China Pursuing Counter-Intervention?,” The Washington Quarterly, Volume 38, Issue 3, Pages 143-156, DOI: 10.1080/0163660X.2015.1099029.

よって今なお主に構成されている[3]。しかし、中国の対介入戦略を可能にする最も重要な要素は、世界最大のロケット軍と、新たな軍事宇宙部隊である。軍事宇宙部隊は、宇宙ベースのセンシング能力と対宇宙能力を追求すると考えられ、廃止された戦略支援部隊の一部に取って代わっている[4]。

---

[3] 例えば、PLAAF は、米国の 500 機を超える空中空輸機数に比して、僅かに約 2 ダース（24 機）を運用するに過ぎない。次を参照。Caleb Egli, “Fueling a Superpower: Reprioritizing the US Air Refueling Fleet for Great-Power Conflict,” Air University, May 8, 2024, https://www.airuniversity.af.edu/JIPA/Display/Article/3768313/fueling-a-superpower-reprioritizing-the-us-air-refueling-fleet-for-great-power/; Mike Yeo, “Satellite Images Suggest China’s New Tanker Aircraft Is under Production,” Defense News, February 18, 2021, https://www.defensenews.com/global/asia-pacific/2021/02/18/satellite-images-suggest-chinas-new-tanker-aircraft-is-under-production/.

PLAN は、攻撃と防御を行える次の主要な戦闘部隊から成る。

- 小型の航空母艦（欧州の CV（航空母艦）に相当）3 隻。これに対し米国はより大型の原子力空母 11 隻。
- 強襲揚陸艦 3 隻。これに対し米国は強襲揚陸艦 10 隻。
- ドック型輸送揚陸艦 8 隻。これに対し米国はドック型輸送揚陸艦 23 隻。
- 巡洋艦 8 隻。これに対し米国は巡洋艦 10 隻。
- 攻撃型原子力潜水艦 6 隻。これに対し米国は攻撃型原子力潜水艦 50 隻。
- 駆逐艦 25 隻。これに対し米国は兵器搭載容量が 50%多いアーレ―バーク級駆逐艦 70 隻。

より小規模な戦闘部隊では、PLAN は次から成る。

- PLAN フリゲート艦 30 隻。これに対し米国は同様の沿海域戦闘艦 32 隻。
- 静粛性のある 039A 型通常動力型潜水艦（元型）24 隻。第 2 列島線の外では静粛性を維持して稼働することはできない。
- より旧式の通常動力型潜水艦約 24 隻。
- 中程度の係争環境で自衛に必要な容量の兵器のみを有する、より旧式のフリゲート艦と駆逐艦約 24 隻。米国には同等の退役艦がある。

次を参照。Office of the Secretary of Defense, *Military and Security Developments Involving the People’s Republic of China*, (Washington DC: US DoD, 2023), https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARYAND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[4] Namrata Goswami, “The Reorganization of China’s Space Force: Strategic and Organizational Implications,” *The Diplomat*, May 3, 2024, https://thediplomat.com/2024/05/the-reorganization-of-chinas-space-force-strategic-and-organizational-implications/; Office of the Secretary of Defense, *Military and Security Developments Involving the People’s Republic of China*, (Washington DC: US DoD, 2023), https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

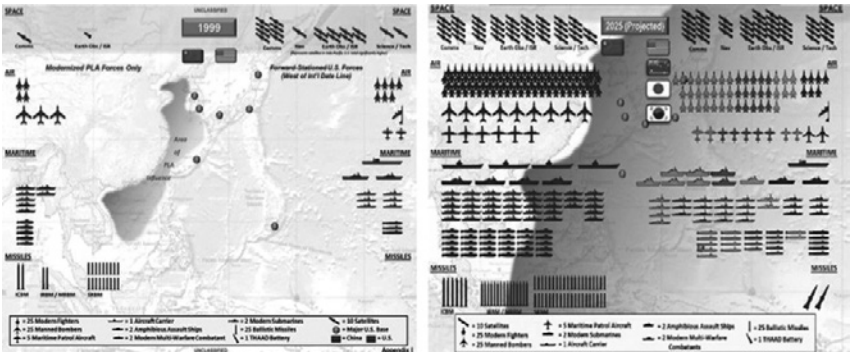


図１：西太平洋における PLA の態勢と地域配備の米軍及び同盟国軍との比較[5]

また、PLA は将来の衝突において「ホームチーム」となる可能性が高いことから、PLA の指導者たちは米軍に対抗するための構想と能力の開発に集中できるという余裕のある状況を得ている。図１に示すとおり、PLA は日本、台湾、豪州、韓国からの軍隊に対抗する可能性があるが、こういった米国の同盟国は米国のシステムに大きく依存しており、また相互運用性向上のため米国の戦術を模している。紛争においては、PLA はこれら同盟国の本国を攻撃することにより、同盟国による貢献を更に弱体化させることができる。なぜなら、同盟国の指導者たちは、本国の防衛に集中させるために比較的小規模な軍隊を撤退させざるを得ないからである。

紛争抑止のためのセンシングとセンスメイキングの劣化

中国の侵略を抑止するために、米軍は西太平洋において持続可能で残存可能な軍の態勢を導入する必要があると考えられる。軍事侵攻のように、急速に展開する大規模な紛争では、PLA が米国や同盟国における多数の目標を同時に攻撃しようとすれば、PLA の打撃能力は弱くなる。封鎖のような、長期的かつ烈度の

[5] Brian Everstine's post on X, September 14, 2020, https://x.com/beverstine/status/1305512270571745282.

低いシナリオでは、PLA は個々の目標に対しより多くの兵器を使用できる。加えて、台湾シナリオとは異なり、争いが戦域レベルに進展しない限り、米軍は中国本土に反撃することはできないであろう。

西太平洋における PLA との対称的なミサイル対防空の競争において、国防総省が優位に立つ可能性は低い。むしろ、非対称的なアプローチを取り、同盟国による作戦を PLA が理解し予測する能力や、米軍を正確に狙う能力を劣化させる必要がある。敵対者の指揮・統制・通信・情報・監視・偵察（C3ISR）を攻撃することは、既に米インド太平洋軍の指導者たちが目標として表明している[6]。しかしながら、歴史的に見て、対 C3ISR 作戦は、戦闘中に敵の攻撃を打破することに焦点を当てているが、PLA の能力の優位性により、米国と同盟国による電磁戦（EW）やサイバー作戦が阻止される可能性がある。米国と同盟国の対 C3ISR 作戦は、むしろ紛争防止に焦点を当てる必要があろう。PLA の指揮官は、米国と同盟国の部隊による当該地域での行動を目にするかもしれないが、正確な位置情報を取得できない場合、米国や同盟国のどの部隊が計画される作戦において最も重要かが予測できない場合、又は狙った目標に PLA の兵器が正確に命中する見込みがない場合には、PLA は攻撃を断念する可能性がある。

PLA のセンシングとセンスメイキングを攻撃するというこのアプローチは、PLA の作戦構想である「システム体系戦」に内在する脆弱性を利用しつつ、米国の C3ISR 能力、サイバー効果、EW 効果における米国の強みを利用するものである。図 2 に簡潔に示すとおり、「システム体系戦」は偵察・情報システム、火力打撃システム、指揮システム、支援システム、情報対峙システムによる作戦を組み合わせ、PLA の計画担当者が米軍のシステム体系における主要な脆弱点であると評価したものを攻撃する[7]。

PLA による「システム体系戦」の採用は、精密誘導打撃戦という米国が成功

6　Jon Harper, “Counter-C5ISRT is Top Priority for Nominee to Lead Indo-Pacific Command,” DefenseScoop, February 1, 2024, https://defensescoop.com/2024/02/01/counter-c5isrt-samuel-paparo-indo-pacific-command-nomination/.

7　Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare* (Santa Monica, CA: RAND, 2018), https://www.rand.org/pubs/research_reports/RR1708.html.

したアプローチを模す試みとの側面もあるが、それに中国特有の特徴を加えたものである。米国の作戦は基本的に遠征作戦であるが、PLA の作戦は主として局地的である。戦闘中においては通信の維持が困難であることから、米国の上級士官及び政治指導者は、発射順序の決定、作戦行動の指揮、及び新たに生じる機会の活用といった作戦管理を現地の指揮官に頼ることが多く、これにより初動における優位を獲得する。対照的に、ほぼ全ての PLA 部隊（PLA ロケット軍（PLARF）、PLAAF 等）は中国国内に拠点を置いていることから、トップの PLA 指揮官及び中央軍事委員会（CMC）は PLA 部隊と容易に通信を行うことができる。これにより上層部は作戦を直接管理することができ、現地の指揮官に頼る必要がなくなる。なお、中国の上級士官は現地の指揮官を有用又は忠実であると信じていない可能性がある[8]。

ヒエラルキー型の性質を持つ PLA の指揮・統制（C2）により、偵察・情報システム及び火力打撃システムは、PLA の「システム体系戦」の最も重要な要素となっている[9]。PLAの指導者たちは、広範囲にわたる宇宙、地上、空中、及び海上配備システムから送信されるセンサーデータを統合する偵察・情報システムに依存している。その後、同データは長距離精密打撃のため、中国領土内又はその付近のミサイル発射装置に提供される。

---

[8] Jackson, Kimberly, Andrew Scobell, Stephen Webber, and Logan Ma, *Command and Control in U.S. Naval Competition with China*, (Santa Monica, CA: RAND Corporation, 2020), Pages 23-49. https://www.rand.org/pubs/research_reports/RRA127-1.html; Larry Wortzel, "The PLA and Mission Command: Is the Party Control System Too Rigid for Its Adaptation by China?," Association of the US Army, March 2024, https://www.ausa.org/sites/default/files/publications/LWP-159-The-PLA-and-Mission-Command-Is-the-Party-Conrol-System-Too-Rigid-for-Its-Adaptation-by-China.pdf.

[9] Joel Wuthnow, "System Destruction Warfare and the PLA," Institute for National Strategic Studies, June 2024, https://keystone.ndu.edu/Portals/86/PLA%20Systems%20Attack%20-%20JW%20update%20June%2024.pdf.

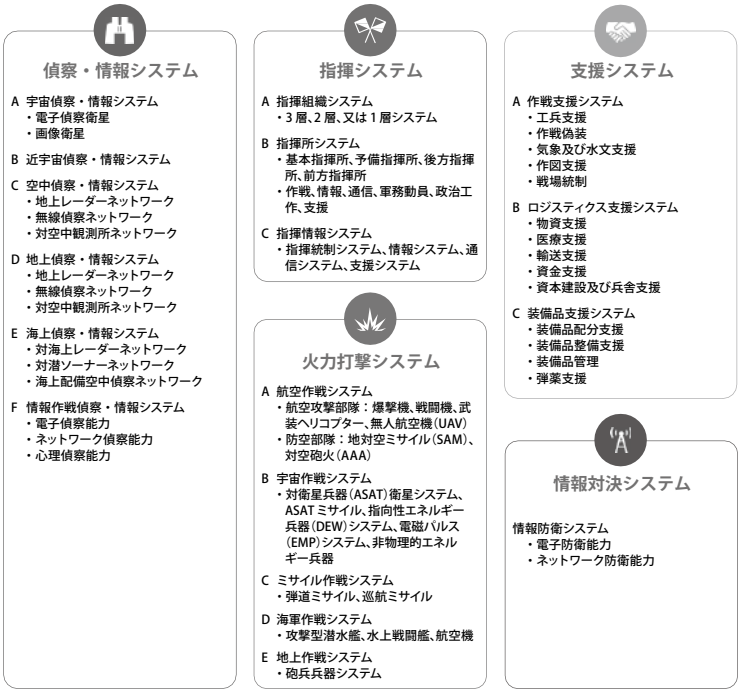


図 2：PLA システム体系戦構想の概略

この中央集権的な構造によって、米軍と同盟国軍が PLA のセンシングとセンスメイキングを弱体化させることにより、優位性を獲得する機会が生じる。PLA の航空機と艦艇からの情報は複数のデータリンクにより送信されると考えられ、これによりレイテンシーが増大し、信頼性が低下すると考えられる。地上及び宇宙ベースのセンサーデータは、主に有線接続によりセンサーや地上局から司令部に伝達されると考えられ、航行中の艦艇や航空機に比べ、適時性と強靭性が大きくなる。しかし、いずれの種類のセンサーも、PLA の作戦状況図や意思決定を混乱させ得るジャミング、欺瞞、及び通信阻止に対し脆弱である。

センシングの混乱と劣化

米軍と同盟国軍は、地表及び上空において何十年にもわたって行われてきた、PLA センサーに対する EW とサイバー作戦の経験を活用することができる。センサーは全て無線周波数（RF）、可視光、又は赤外線（IR）放射に依存しているため、偽の信号や不明瞭化する機能を有する信号、悪意のあるコンピューターコードに対し脆弱である。ハドソン研究所による過去の報告書で説明されているとおり、ソナーのような海中センサーは音響に依存しているため、同様に操作し、PLA の海底作戦状況図を妨害することができる[10]。

同盟国は、巧みに統制された取組で PLA のセンサーを欺く又は妨害することにより、PLA の作戦状況図や計画を混乱させられる可能性がある。しかし、これらの取組が成功する期間は限られている。効果的な対センシング作戦のためには、同じ地理的な位置や目標を扱っている複数のセンサーからの出力を偵察・情報システムがリアルタイムで組み合わせる可能性について対処する必要があろう。人工知能（AI）対応アルゴリズムの助けを得て、センサーフュージョンや人間のオペレーターを活用することにより、最終的には同盟国軍の真の位置や活動を決定できるようになるであろう。

敵対者のセンスメイキングに対する攻撃

そのため、同盟国軍は、PLA のセンスメイキングを攻撃することにより、PLA のセンサーフュージョンの劣化を図る取組を補完する必要がある。一つの方法は、あらゆるドメインにおける複数のセンサーからの出力を同時にまとめるために必要な通信ネットワークを妨害することである。合成開口レーダー（SAR）航空機からのデータリンクのような信号へのジャミング又は割り込みがあった場合、偵察・情報システムのセンサーフュージョン能力は明らかに劣化する。また、データリンク

---

[10] Bryan Clark and Timothy A. Walton, *Fighting into the Bastions: Getting Noisier to Sustain the US Undersea Advantage*, (Washington, DC: Hudson Institute, 2023), https://www.hudson.org/fighting-bastions-getting-noisier-sustain-us-undersea-advantage-submarine-bryan-clark-timothy-walton.

へコードを挿入してメッセージフォーマットを変更する等、より巧妙な手法を用いれば、センサーデータの統合を遅らせたり、データが他の場所や目標に関連しているように見せかけたりでき、その結果センサーフュージョンを挫くことができると考えられる。

米軍と同盟国軍はまた、対センシング作戦を予測困難な戦術や兵力構成と組み合わせることにより、PLA のセンスメイキングを弱体化させることができる。偵察・情報システムの AI 対応アルゴリズムは、PLA の行動方針（COA）策定のための情報を提供するため、センサーデータと過去の米国の作戦やドクトリンとの比較を試みる。米軍と同盟国軍が、PLA によって既に確認及び研究済みのものだけというよりは、むしろ幅広い兵力構成や作戦構想を追求する、という可能性を確立することにより、PLA の AI 及び予測計画プロセスへの依存を利用することができる。

国防総省の現在の連合統合全領域指揮・統制（CJADC2）における取組は、作戦行動の組立てや統制において指揮官により多くの選択肢を与えられるような、より再編可能な戦力を実現する一助となる。陸軍のプロジェクト・コンバージェンスや海軍のプロジェクト・オーバーマッチにおいて進められた実験により、通信相互運用性の向上を通じて、米軍が利用可能なキルチェーンの多様性が増している。戦闘軍司令官レベルでは、CJADC2イニシアティブにより、統合火器ネットワーク（JFN）が初めてインスタンス化された。JFN は戦域全体にわたり指揮官、シューター、センサーをつなぎ、調節可能な一連の攻撃の選択肢を提供することになる[11]。

しかしながら、より幅広い COA を指揮官にもたらし、その結果、敵のセンスメイキングに対してもたらす不確実性がより大きくなるという点においては、通信の相互運用性よりも戦力設計の方が大きな影響を及ぼし得る。図 3及び筆者のモザイク戦及び意思決定中心戦に関する研究において説明しているとおり、国防

[11] Mark Pomerleau, “Indo-Pacific Command to Test Prototype of Joint Fires Network This Year,” DefenseScoop, March 21, 2024, https://defensescoop.com/2024/03/21/joint-fires-network-indo-pacific-command-test-prototype/.

総省は、PLAのセンスメイキングを実質的に劣化させるための戦力は、機能を少なくし（無人もあり得る）、部隊の数を増やし、細分化する必要があると考えられる。図3の上部に示している小規模な戦力は、構成手法の数が限られるため、狭い範囲の作戦構想及び戦術にしか対応できない。複数任務の艦艇や航空機から成る小規模な戦力であっても、PLAのような対戦相手にとっては、実質的な複雑さをもたらすとはいえない。各プラットフォームが多くの場合自己充足型のキルチェーンとして機能することから、たった一つの目標を攻撃するだけで無力化されるためである。

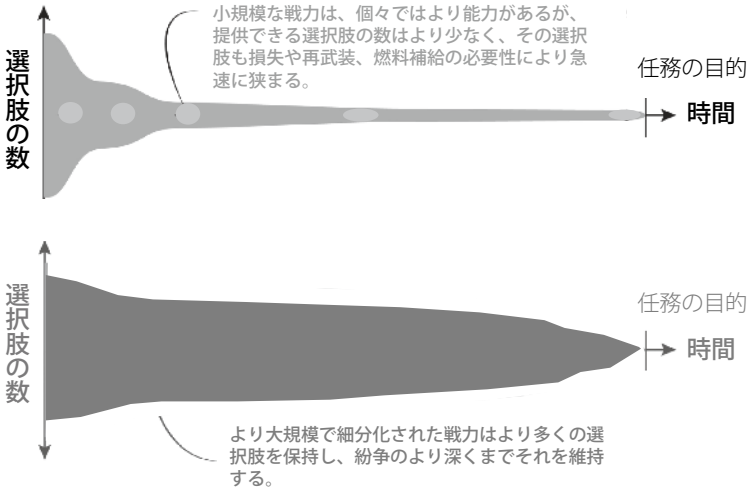


図3：同盟国指揮官が取り得る選択肢

多数の個別部隊を含む大規模な戦力は、より小規模な戦力よりも洗練の程度は低いとしても、指揮官にとってはキルチェーンを構成する選択肢の数が増えると考えられ、そのためPLAのセンスメイキングに対しより困難な状況を生み出すと考えられる。また、細分化を有用なものとするのに、実際の兵器システムを用いる必要はない。デコイ又は模擬のプラットフォームや車両により、実物と同じように敵のセンスメイキングを複雑にすることができ、それにより敵対者は、より幅広

い米国の選択肢に備えるか、センサー情報の曖昧さを解消するために時間とセンシング資源を費やすことを迫られる。

クロスドメイン非物理的効果の重視

20世紀の戦争や21世紀のテロ対策に比べ、大国の包括的なセンシング及びセンスメイキング・アーキテクチャを弱体化させるには、米軍と同盟国軍には、より洗練されたEW及びサイバーアプローチが必要となろう。従前の対立においては、非物理的能力は、各々のドメインの中における紛争の異なる段階で使用されることが多かった。サイバーエクスプロイトやマルウェアは、平時における情報作戦やテロ対策作戦の一環として作成され、有線回線を介して展開されることが多かった。EWジャミングや偽目標は、戦闘中に敵のレーダーや無線通信にRFスペクトラムを通じて送信された。例えば、PLAの偵察・情報システムの大部分は、中国国外からはアクセスできない独立型ネットワーク上に構築されており、多くの冗長性のあるRFセンサーを組み入れている。

敵対者がデジタル技術を通信とセンシングに組み入れている場合、同盟国軍にとっては、強靭なセンシング及びセンスメイキングネットワークを作ろうとする敵対者の取組を防ぐ機会が生まれる。コンピューター制御の軍事センサーは、信号処理によりEW攻撃を検知し反撃するのには優れているが、デジタルシステムにおいては、共通のセキュリティ上の弱点も存在する。また、潜在的対戦相手は、ハッキング対策のために軍事通信における独立型ネットワークの使用を増やしたものの、センシング、及びセンサーの相関やフュージョンを可能にするための宇宙、空中、及び海上配備のプラットフォームとの通信においては、今もなおRFアパーチャに依存している[12]。

---

[12] Mark Pomerleau, “Services Working to Convergence EW, Cyber Warfare Capabilities,” DefenseScoop, September 30, 2022, https://defensescoop.com/2022/09/30/services-working-to-convergence-ew-cyber-warfare-capabilities/.

図４及び2020年国防総省「電磁スペクトラム優勢戦略」[13]に示されているように、これが示唆していることは、敵対者によるセンサー処理とフュージョンに打ち勝つためには非物理的効果を一層組み合わせる必要があるということである。例えば、従来のように「ネットワーク上の」サイバー効果を有線接続によりもたらすことに加え、RFアパーチャを通じて独立型ネットワーク内にもサイバー効果をもたらす必要があろう[14]。センサーや無線通信に到達するRF信号を操作したり不明瞭にしたりする従来のEW効果に加え、EW効果は、受信者による処理やEW効果が成功したか否かの検証作業を劣化させるサイバーエクスプロイトに依存することになろう[15]。

図４：非物理的効果間の新たな関係

サイバー対応EWやRF対応サイバー作戦のような攻勢的なクロスドメイン非物理的効果により、国防総省のC2に新たな考えがもたらされている。ネットワー

---

[13] US DoD, *2020 Department of Defense Electromagnetic Spectrum Superiority Strategy* (Washington, DC: US DoD, 2020), https://dodcio.defense.gov/Portals/0/Documents/Spectrum/2020DoD-EMS-SuperiorityStrategy.pdf.

[14] Director, Operational Test and Evaluation (DOT&E), *Cyber Assessment Program (CAP)* (Washington, DC: US DoD, 2023), https://www.dote.osd.mil/Portals/97/pub/reports/FY2023/dotemanaged/2023cap.pdf?ver=DrwfdCEmkKW0KX4UEQLFXg%3D%3D#:~:text=DoD's%20cyber%20posture%20remains%20at,systems%20that%20are%20essential%20to.

[15] Mark Pomerleau, "US Cyber Command Looking at How to Utilize Tactical On-the-ground Systems," DefenseScoop, January 16, 2024, https://defensescoop.com/2024/01/16/us-cyber-command-looking-at-how-to-utilize-tactical-on-the-ground-systems/.

ク上の米国の攻勢的サイバー作戦は、通常、運用レベルから戦略レベルにおいて、米軍サイバーコマンドのような戦闘軍司令官や国家指揮権限者（大統領又は国防長官）により認可される。このことは、サイバーツールの使用により、付帯的損害が即座かつ反復して生じる可能性があるという永続的な影響があることを反映している。攻勢的 EW 作戦は、通常、現地の指揮官や個々のオペレーターにより戦術レベルから運用レベルで統制されているが、これはその効果が一時的であり、目標とされたアパーチャに限定されていることによる。サイバー作戦と EW 作戦の双方における防勢的な効果は、ほぼ常に、それよりもかなり低いレベルの権限で統制されており、自動化されていることが多い。

クロスドメイン非物理的作戦の刷新

攻勢的なクロスドメイン非物理的効果は、新たな C2 アプローチを必要とする。他の軍事作戦と同様、非物理的効果をもたらすオペレーターは目標へのアクセスを必要とするが、大抵は一瞬でなされる。ネットワーク上のサイバー効果のためには、通常、上層部がリアルタイムで大陸間の距離で目標を監視し、適時に実行を許可することができる。対照的に、サイバー対応 EW や RF 対応サイバー効果をもたらす部隊は、大抵、司令部から遠く離れた通信がつながりにくい地域に置かれている。そのため、現地の指揮官は、目標となるアパーチャがアクセス可能な時間内に上層部からの許可を得るのが困難となる可能性がある。

また、クロスドメイン非物理的効果は、従来のサイバー効果や EW 効果とは異なるタイムスケールで起こるため、計画と実行が複雑になる。一たび許可されると、オペレーターはネットワーク上のサイバーツールを光速で送ることができ、その影響は数分から数時間続く。ジャミングやデコイの使用のような EW 作戦は数分から数時間行われるが、その理由は、効果が一時的であることと、通常は EW システムが止められれば消散することである。EW 作戦のように、クロスドメイン非物理的効果の場合、適切なアパーチャへのアクセスが困難なために数分から数時間を要することがあるが、デジタルコードを含むことから、その影響はサイバー効果のように長時間にわたる可能性がある。サイバー対応 EW 及び RF 対応サイ

バー効果については、他の軍事能力の導入方法と同様、ハイブリッド型 C2アプローチが必要となろう。サイバー効果がインターネット上に存在することにより付随的損害を引き起こしたり、「野に放たれる」のを許したりすることから、軍及び文民の上層部は通常、ネットワーク上のサイバー効果をコントロールすることを好む。しかし、クロスドメイン非物理的効果は、実質的に隔絶された敵対者に対し使用され、他の軍や民間のネットワークに影響を与える可能性は低い。サイバーや EW における米の優位性を利用する機会を逸することがないよう、上層部はクロスドメイン効果の種類やカテゴリーを承認するとともに、現地の指揮官に対し、所定の交戦規定に従って使用する権限を委任することが考えられる。

本報告との関係で最も重要な点として、クロスドメイン非物理的効果においてもまた、新たな能力開発アプローチが必要になる。米軍と米国サイバーコマンドは、軍事作戦に使用される頻度が低いことから、政府所有の「射場」において、比較的遅い速度で新たな攻勢的サイバーツールを開発している。対照的に、各軍は EW 要件開発やプログラムの修正のための堅固なインフラを有しており、時間はかかるものの、毎年、かなりの数の変更を行っている。国防総省には、有線ネットワークと RF デリバリーメカニズムの双方をモデル化し、電磁環境とサイバー環境にわたり活動を統合できるアプローチが必要となる。

国防総省による非物理的能力開発プロセスはまた、今日よりもその規模を拡大する必要があると考えられる。米軍は、平時の競争や危機の際、非物理的効果を使用する頻度を増やす必要がある。歴史的にはこのような作戦は戦闘時に限られており、同盟国軍の防護や敵の攻撃の実効性を低下させるために行われた。しかしながら、戦略地政学的に不利な状況により、諫止（dissuasion）と抑止（deterrence）の一部として、米軍と同盟国軍は敵のセンシングとセンスメイキングを妨害する必要があると考えられる。PLA が展開しているような能力への対センシング及び対センスメイキング・キャンペーンに対するアプローチについては後に詳述する。

国防総省は、対センシング及び対センスメイキング・キャンペーン実施のために、非物理的効果の「分厚い弾倉」を必要とするであろう。対センシング及び対センス

メイキング・キャンペーンに必要な規模と速度で非物理的能力を開発するために国防総省がとり得るアプローチについて説明した上で、最後に、国防総省がこの新たなプロセスを採用し、米軍がポスト・ドミナンス期において優位を取り戻すための提言を行い、本報告を締めくくる。

2. 抑止と諫止のための対センシング及び対センスメイキングの活用

同盟国軍は、抑止が失敗した後になってから戦闘中にC3ISR能力や対C3ISR能力に頼るよりも、抑止と諫止を支援するためにこれら能力における優位性を活用すべきである。従来、米軍は、敵対者の攻撃の成功を拒否すると脅したり、攻撃による利益を上回るような経済的・軍事的な懲罰を課したりすることで、抑止を追求してきた。ポスト・ドミナンス期においては、このアプローチは効力をなくしつつある。ロシアのウラジーミル・プーチン大統領は、第二次世界大戦以降最も包括的な経済的・外交的な懲罰に直面しても、2022年にウクライナを攻撃することを選択し、ウクライナが当初の急襲を持ちこたえた以降も侵攻を継続した[16]。イランに支援されたフーシー派反政府勢力は、イランに対する制裁や米軍と同盟国軍による反撃があったにもかかわらず、中東全域において米国の地上部隊や海軍部隊を定期的に攻撃している[17]。また、中国海警局及び海上民兵組織は、フィリピン、台湾、日本の海軍や警察部隊に対し恒常的に嫌がらせをしたり、周期的に衝突を起こしたりしている[18]。

米国とその同盟国は、中国の攻撃を諫止するためには、懲罰的脅しや拒否以上

---

16 Nadia Schadlow, “Why Deterrence Failed Against Russia,” The Wall Street Journal, March 20, 2022, https://www.wsj.com/articles/why-u-s-deterrence-failed-ukraine-putin-military-defense-11647794454.

17 Oren Liebermann and Nikki Carvajal, “Biden Concedes Houthis Haven’t Been Deterred from Carrying Out Attacks as US Launches Further Strikes,” CNN, January 18, 2024, https://edition.cnn.com/2024/01/18/politics/biden-houthi-strikes/index.html.

18 Derek Grossman, “How to Respond to China’s Tactics in the South China Sea,” *Foreign Policy*, May 29, 2024, https://foreignpolicy.com/2024/05/29/philippines-us-south-china-sea-gray-zone-tactics-alliance-military-treaty/.

のことをする必要があろう。ロシアのウクライナ東部における「グレーゾーン」作戦やクリミア併合のような漸進的な攻撃に対しては、従来の軍事力では対抗が困難な可能性がある。ロシアによる2022年ウクライナ侵攻のような、よりあからさまな行動の方が認識しやすいものの、猶予なく長距離から阻止することは困難である。中国の台湾封鎖は前者に近いと思われ、侵攻は後者により近いといえよう。

米軍と同盟国軍は、中国の偵察・情報システムへの依存を利用し、双方の種類の課題に対処することが考えられる。例えば、封鎖を実行している中国軍は、封鎖されている国への船舶による出入り地点及び護衛している可能性がある艦艇の位置を把握するために、正確かつ時宜を得た作戦状況図を必要とする。台湾侵攻の際、攻撃を行う中国軍は、ウクライナで起きたように紛争が長引いた場合に後で必要となり得る兵器を無駄にしないよう、目標に関する正確な情報が必要となる。

2022年の米国の国家防衛戦略（NDS）は、「キャンペーニング（campaigning）」のための努力の集中（line of effort）を通じてPLAのセンシングとセンスメイキングの弱点を利用する方法について提案している。「部隊を運用し、国防総省の広範な取組を同期させ、国防総省の活動を国力の他の形態と同期させ、競争相手による重大な強制を弱体化し、競争相手の軍事的準備を複雑化し、同盟国やパートナーと共に我々の作戦能力を強化する」ことを同戦略は国防総省に対し指示している[19]。

米国海兵隊のドクトリンでは、キャンペーニングは特定の時間と空間で特定の目的を達成するために設計された一連の作戦である[20]。キャンペーニングでは、多くの歴史的な事例が裏付けているように、戦闘の勝利は長期的目的の達成を保

---

[19] Lloyd Austin, *2022 National Defense Strategy of the United States of America*, (Washington, DC: US DoD, 2022), 1, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

[20] US Marine Corps, "Campaigning," in *Marine Corps Doctrinal Publication 1-2*, August 1, 1997, https://www.marines.mil/Portals/1/Publications/MCDP%201-2%20Campaigning.pdf.

証するものではないことを認識している[21]。キャンペーンは、第二次世界大戦中の連合軍による欧州奪還のように大規模な戦闘作戦と関連付けられることが多いが、マレーシアにおける英国の対反乱作戦のように、長期にわたる強度の低い活動でも構成される場合がある[22]。上記及びその他のキャンペーンの成功には非軍事手段も大きな役割を果たしているが、本報告では軍事活動の適用に焦点を当てる。

国防総省は、中国の攻撃を諫止するために、対センシング及び対センスメイキング・キャンペーンを利用することができる。抑止ほど研究・議論はされていないが、紛争が差し迫っていない場合には、諫止は競争や対立に影響を与える手段を提供する。戦闘員が戦争に向け突き進み、主要な決定が既になされている場合には、それを止めるには失敗の確実性か耐え難い懲罰しかない可能性が高いが、そうでない場合、諫止の努力により、敵対者が破壊的な行動に向かわないようにできる可能性がある[23]。

エスカレーションの優位性の回復

中国の軍と準軍事組織は、台湾侵攻を支援するためには、激しくかつ大規模な火力キャンペーンを開始する必要があろう。歴史が示すように、水陸両用強襲は高いリスクを伴う作戦であり、多数の部隊を長期にわたり脆弱な状態にさらす

---

[21] 恐らくこの最も良い例はウィリアム・ウェストモーランド（William Westmoreland）であり、多くの人はベトナム戦争において米国は目的を達成できなかったと考えているが、米軍は戦った全ての戦闘に勝利したのだと傲然と主張した。次を参照。Neil Sheehan, *A Bright Shining Lie: John Paul Vann and America in Vietnam* (New York: Random House, 1988).

[22] Robert W. Komer, *The Malayan Emergency in Retrospect: Organization of a Successful Counterinsurgency Effort* (Santa Monica, CA: RAND, 1972), https://www.rand.org/pubs/reports/R957.html.

[23] このアプローチの詳細は、次を参照。Bryan Clark and Dan Patt, *Campaigning to Dissuade: Applying Emerging Technologies to Engage and Succeed in the Information Age Security Competition*, (Washington, DC: Hudson Institute, 2023), https://www.hudson.org/defense-strategy/campaigningdissuade-applying-emerging-technologies-engage-succeed-information-age-bryan-clark-dan-patt.

ことになる[24]。台湾やその同盟国が侵攻軍を阻止するのを防ぐために、PLA は東シナ海、南シナ海、フィリピン海の全域で艦艇、航空基地及び航空母艦を無力化する必要があろう。PLA の火力を低下させると侵攻が失敗する可能性が高まるため、米軍と同盟国軍は対センシング及び対センスメイキング作戦を用いることが考えられる。

通常、PLA は台湾及びその同盟国よりも実質的なエスカレーションの優位性がある。図 5 に示すとおり、偵察・情報システムと火力攻撃システムにより、PLA は近傍において、自らのグレーゾーン作戦の防衛を含め、様々な規模で大量の火力攻撃を行うことができる。同盟国軍は PLA の攻撃から自らを守る防衛能力を欠いており、同盟国軍が結集して大編成となればその限りではないが、これが現実的なのは大規模な紛争の場合のみであろう。加えて、同地域の米軍と同盟国軍は、グレーゾーンの対立への対応としての大編成は、過度に挑発的又はエスカレーションを引き起こすものであると考える可能性がある。

図 5 に示す非対称性により、米軍と同盟国軍は中国よりもエスカレーションにおいて不利である。例えば、中国の海上民兵組織と中国海警局船艇は、中国本土からの艦艇、航空機、防空、及び地対地ミサイルによる防護の下、フィリピンの漁船や沿岸警備船艇に対する嫌がらせや衝突を行うことができる。攻撃に直面した同盟国軍は、高いリスクを冒して対抗するか、あるいは、生存のため及び反撃の脅しのために、相当量の攻撃的・防御的火力を中国に近い激しい係争環境の中に持ち込む必要があると考えられる。しかし、そのような断固とした軍の態勢は、攻撃者は中国というより米軍と同盟国軍であるかのように見せることになり、逆効果となる可能性がある[25]。

---

[24] Carter Malkasian, *Charting the Pathway to OMFTS: A Historical Assessment of Amphibious Operations from 1941 to the Present*, (Alexandria, VA: CNA, 2002), https://www.cna.org/reports/2002/D0006297.A2.pdf.

[25] こういったダイナミックな解決策案については、次で取り扱われている。Bryan Clark, Mark Gunzinger, and Jesse Sloman, *Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance,* (Washington, DC: CSBA, 2017), https://csbaonline.org/research/publications/winning-in-the-gray-zone-using-electromagnetic-warfare-to-regain-escalation.

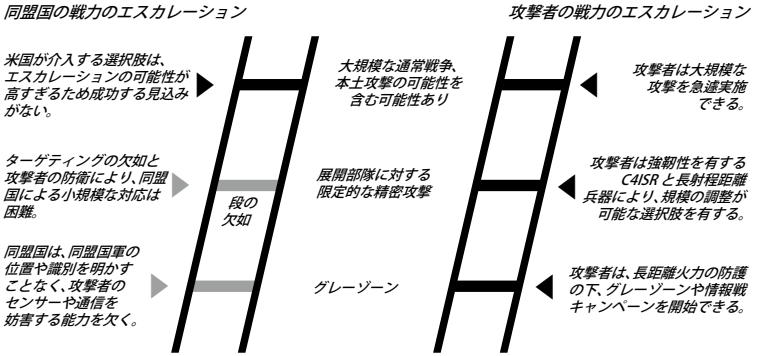


図 5：同盟国軍（左）と PLA 軍（右）のエスカレーションラダーの比較

適切なデリバリーシステムと効果があれば、米軍と同盟国軍は、図 6に示すように、非物理的作戦を用いてエスカレーションラダーの下方における複数の段（rungs）を回復し、非対称性を転換することができる。例えば、米軍と同盟国軍は、ジャミングにより敵対者のセンサーを劣化させるとともに、電磁スペクトラム（EMS）の複数の領域にわたり長期間持続するデコイを展開することができる。米軍と同盟国軍は、センスメイキングを複雑にする行動により、対センシング作戦の影響を拡大できる。例えば、敵対者のオペレーターが過去のパターンに基づき、どの目標が本物であり最も価値があるかを判断する機会を拒否する分散型かつ再構成可能なフォーメーションを用いることができる。敵対する指揮官の計画に不確実性を生み出すことに加え、こういった行動は敵対者の偵察・情報システムの有効性に関する懸念を明らかにする反応を引き出す可能性がある。

非物理的効果はまた、潜在的な攻撃者をより高いレベルのエスカレーションへ引き上げると考えられる。米国と同盟国による対センシング及び対センスメイキング作戦に直面する中、意図した目標を確実に攻撃するため、全ての潜在的な目標を同時に攻撃すべく、より多くの兵器を使用する必要が生じる可能性がある。あるいは、敵の指揮官は目標の情報を更に明確にしてより効率的な攻撃を試みる可能性もあるが、こうした行動もエスカレーションを引き起こす可能性がある。PLA

は、正確な類識別情報を取得するため、又は火器管制レーダーで照射するために、米軍と同盟国軍にセンサープラットフォームを相当接近させる必要がある可能性があるが、これは挑発的と捉えられ得る。いずれにしても、対センシング及び対センスメイキングは、中国のエスカレーションラダーから下の方の複数の段を取り除くことになる[26]。

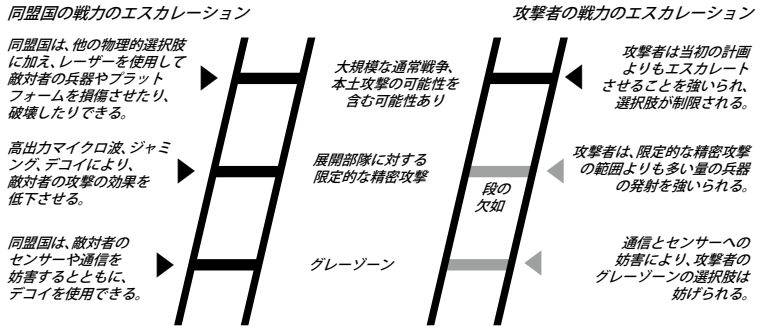


図６：効果的な対センシング及び対センスメイキング（左）がある場合の修正エスカレーションラダー

対センシング及び対センスメイキングはまた、それ自体がエスカレーションの選択肢であることに加え、同盟国が小規模な物理的攻撃を実施する能力を回復させると考えられる。図６に示す現在のエスカレーションパラダイムにおいては、海上民兵組織の船舶を無力化する、あるいは侵入してきた爆撃機を強制着陸させるといった小規模攻撃は、中国周辺地域では高いリスクを伴う。しかしながら、対センシング及び対センスメイキング作戦で補完することにより、このような小規模攻撃を、作戦完了まで覆い隠したり、中国の指導者がエスカレートの選択をしなくなるほど大規模な介入を要するものであるかのように見せたりすることが可能と考

[26] Bryan Clark and Dan Patt, *Campaigning to Dissuade: Applying Emerging Technologies to Engage and Succeed in the Information Age Security Competition*, (Washington, DC: Hudson Institute, 2023), https://www.hudson.org/defense-strategy/campaigning-dissuade-applying-emerging-technologies-engage-succeed-information-age-bryan-clark-dan-patt.

えられる。

対センシング及び対センスメイキング・キャンペーンの設計

今日の中国と米国の間に存在しているような平時の競争においては、米国主導の対センシング及び対センスメイキング・キャンペーンの目的は、中国の指導者たちを中国の目標へ続く最も破壊的な道から逸らすことであろう。図7に示すとおり、中国は台湾の強制的な統一のために追求し得る複数の異なるシナリオを有している。米国と同盟国から見て最も望ましくない経路は、侵攻、及びそれに続く爆撃や封鎖であろう。

偵察・情報システムを目標にすることにより、対センシング及び対センスメイキング・キャンペーンは、侵攻シナリオにおいて最大の効果を発揮する可能性が高い。台湾やその近隣諸国への空爆は、事前に定められた照準点に依存している可能性があり、封鎖の実施は適時かつ一元的に組織された目標に関する情報に依存しない。対照的に、侵攻を行う際には、PLAの部隊は、侵攻を阻止しようとする可能性がある米国及びその同盟国の水上艦艇、潜水艦及び航空機を迅速に攻撃する必要がある。このような移動中の部隊に事前に照準することはできないが、侵攻を成功させるためには、PLA はこれらを無力化する必要があろう。

対センシング及び対センスメイキング・キャンペーンは、侵攻を実行不可能にするわけではない。PLA には十分な能力の優位性があり、C3ISR のパフォーマンスが貧弱であったとしても成功する可能性がある。しかしながら、侵攻は他のシナリオに比し偵察・情報システムに依存する程度が高いことから、対センシング及び対センスメイキング・キャンペーンにより、中国の指導者たちがそのシナリオを選好する可能性を引き下げ、他のシナリオの方を好むようにする可能性がある。このような他のシナリオも米国及び同盟国の指導者にとっては望ましくないかもしれないが、侵攻に比べれば破壊的ではなく、ペースは遅く、ディエスカレーションへの抜け道をより多く提供する可能性がある。

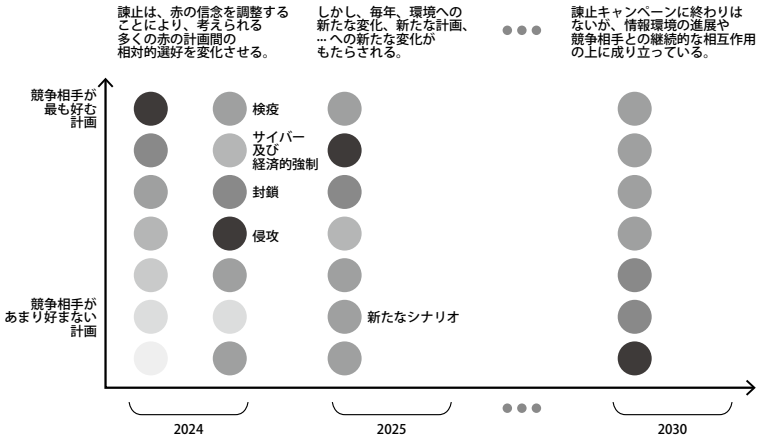


図７：諫止戦略の実施

語れ、見せるな

米国及び同盟国は、ここ数年、エスカレーションラダーの下の方の段をより多く使用している。中国による領空や海域への侵入が増加していることに対し、日本の自衛隊は阻止行動や巡回を強化した。米海軍は、現在、中国が違法に領有権を主張している海域において、豪州、日本、及び欧州の海軍艦艇と共に定常的に「航行の自由」作戦を実施している[27]。そして最も目を引くのは、フィリピンの排他的経済水域内のセカンドトーマス礁やミスチーフ環礁等へのアクセスを阻止しようとする中国の漁船や海警局船艇に、フィリピン船艇がしっかりと対峙していることである[28]。

このようなあからさまな措置は、中国のグレーゾーン作戦に対する同盟国の

[27] Reuters, “Allies, Partners Conduct Joint Naval Exercises in South China Sea for Free and Open Indo-Pacific,” Indo-Pacific Forum, October 4, 2024, https://ipdefenseforum.com/2024/10/allies-partners-conduct-joint-naval-exercises-in-south-china-sea-for-free-and-open-indo-pacific/.

[28] John Pollock and Damien Symon, “China Blocks Philippines Access to South China Sea Reef,” Chatham House, March 21, 2024, https://www.chathamhouse.org/publications/the-world-today/2024-02/china-blocks-philippines-access-south-china-sea-reef.

抵抗を国際社会に示すという点では有効である。しかし、今後の中国のグレーゾーン作戦やエスカレートさせる可能性がより高い攻撃行動を諫止するという点では、逆効果となる可能性がある。中国の指導者たちは恐らく、グレーゾーン作戦は地域覇権を確立し強要する中国の力と決意を示すものと考えており、同盟国が中国の侵入に公然と対抗することにより、その取組は中国の指導者たちにとってのレピュテーションリスクとなる。例えば、フィリピンの船員が座礁した戦車揚陸艦を運用していたセカンドトーマス礁への入り口を中国が閉ざそうとしたのに対し、フィリピンは公然と抵抗したが、これにより中国の指導者たちは、同艦に補給しようとするフィリピンの取組への妨害、嫌がらせ、封じ込めを図る取組を一層強化する必要に迫られる。中国が強力に対応しなければ、中国の指導者たちは、地域内の他国が係争中の領有権の主張について同様の立場をとるリスクを冒すことになる[29]。

秘密裏の行動は、公然の行動よりも、中国の指導者たちに対しより大きな影響を与え得る。図 8 に示すとおり、同盟国軍は中国の指導者たちに対し二つの主要な経路で信号を送ることができる。一つは公然の行動であり、信号は世界の情報環境を通じて敵対者に送られる。もう一つは秘密裏の行動であり、基本的にクローズドフィードバックループの中で一方の競争相手からもう一方へと直接送られる。

[29] Andrew Taffer, “The Puzzle of Chinese Escalation vs Restraint in the South China Sea,” War on the Rocks, July 26, 2024, https://warontherocks.com/2024/07/the-puzzle-of-chinese-escalation-vs-restraint-in-the-south-china-sea/.

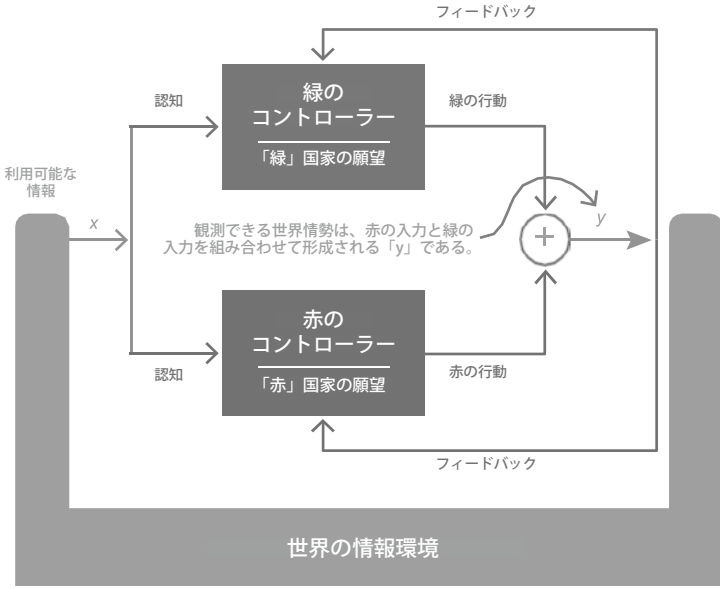


図８：米国及び同盟国（緑）と中国（赤）の間の情報交換

対センシング及び対センスメイキング作戦は、図８のフィードバックループの働きを例示している。敵対者のセンサーや関連したC3能力に影響を与えるよう設計されているため、ジャミング、デコイの展開、サイバー攻撃などの行動を認識するのは、通常は敵対者のみである。場合によっては、商用衛星センシングの事業者などの他者により、対センシング及び対センスメイキング行動が観測される可能性がある。しかし、このような企業や当該企業に依存しているアナリストは、PLAがこの作戦により影響を受けたか否かについては知り得ないと考えられる。中国当局者は、偵察・情報システムの潜在的脆弱性が明らかになることを避けるため、対センシング及び対センスメイキング作戦について不満を述べることは控えるかも

しれない[30]。

中国の指導者たちは同盟国の対センシング及び対センスメイキングの行動を認めないかもしれないが、効果的なジャミングや欺瞞は反応を引き起こすはずであり、PLA のオペレーターはその探知状況を明らかにしようとするとともに、自らのセンサーや C2 能力の脆弱性を修正しようとする。米国及び同盟国の監視者は、中国の反応を用いて、影響を受けたシステム、プロセス、組織が偵察・情報システム全体の中で持つ重要性、及び PLA や中国の指導者たちがシステムの不備に気付いているかについて、評価することができる。例えば、中国の ELINT（電子情報）衛星に対するデコイやジャミング作戦の後に PLA がその軌道を修正しようとしたり、当該地域における ISR 航空機の数を増やそうとし始めたりすれば、同盟国の指導者たちは、ELINT 衛星のパフォーマンスは既に不審なものである、あるいは同衛星は偵察・情報システムの重要なノードとなっている、と評価できる。更なる対センシング及び対センスメイキング作戦では、変更後の ELINT コンステレーションを目標とするか、又は他のセンサーやプロセスへと変更して、これらが偵察・情報システムにおいて果たしている役割を評価することができる。

意外性の弾倉

対センシング及び対センスメイキング行動は、敵対者のターゲティングを劣化させ、その計画を損なうことで、米国及び同盟国の戦闘活動を支援できる。しかし、上記の説明に示されるとおり、非物理的効果は平時の諫止キャンペーンにおいても重要である。この二つの適用は異なる種類のサイバー効果及び EW 効果を必要とし、オーケストレーション（最大の効果を達成しようと試みてイベントを配列すること：訳者注）も異なる。戦闘活動の間、米国及び同盟国は、オペレーターが戦闘時に実行しやすく、他の友軍が観測可能な、標準化された公然の非物理的

[30] Richard Manley, “Cyber in the Shadows: Why the Future of Cyber Operations Will Be Covert,” (Washington, DC: US National Defense University, 2022), https://ndupress.ndu.edu/Media/News/News-Article-View/article/3105355/cyber-in-the-shadows-why-the-future-of-cyber-operations-will-be-covert/.

効果に頼る可能性が高い。しかし、諫止キャンペーンを成功させるには、想定外の効果をもたらす対センシング及び対センスメイキング行動が必要となる。予測可能な同盟国による行動は、「航行の自由」作戦に対する今や当たり前となっている中国の外交上の抗議（demarches）のように、形式的な反応を引き起こすと考えられる。PLAの計画や自信を損ない、中国が自らのシステム、プロセス、組織に対して有する認識について洞察を得るためには、同盟国による非物理的行動は意外性のあるものでなければならない。

平時における対センシング及び対センスメイキング作戦に意外性が必要なことから、このような行動が秘密裏である重要性が増す。中国の国有の商用衛星監視コンステレーションをサイバー攻撃でシャットダウンさせるような、平時において意外性のある公然の行動は、中国指導者にとり、エスカレーションを引き起こす可能性が非常に高く断固とした対応が必要であると映る可能性があり、これは攻撃を諫止するという目標からすると逆効果である。対照的に、中国の指導者たちは、秘密裏の非物理的行動に対しては、実質上の反応をする可能性は低い。強い反応を示せば、攻撃者あるいは更に広範な対象に対し、根底にある脆弱性の存在を認めることになりかねないためである。

非物理的効果により、攻撃の諫止に新たな経路が生じる可能性があるが、同盟国軍にとっては、中国の指導者たちのシナリオ選好に影響を与える規模で、秘密裏かつ意外な非物理的効果を生み出す、という課題が生じる。サイバー効果やEW効果は、それが判明すると、敵対者はC3ISRの脆弱性を速やかに緩和しようとすると考えられることから、通常、長続きしない。平時において競争を継続するには、やがて何千もの非物理的効果を要すると考えられるが、通常兵器と異なり、各々の非物理的効果は異なるものである必要がある。このことは、国防総省は適応性のある効果を大量に生み出せるよう、インフラに投資する必要があることを示唆している。

図9に示すように、同盟国がEW又はサイバー活動を行い、敵対者が対抗策を展開したり、関連する脆弱性を発見、修正したりするに従い、同盟国の非物理的効果の弾倉は急速に消耗する。同時に中国は、同盟国による更なるサイバー攻

撃及び EW 行動を抑止するため、同盟国の利益に対し非物理的行動をとる可能性が高い。米国と同盟国の指導者たちが自信を持って競争を継続し、中国の指導者たちに対して PLA がセンシング及びセンスメイキングの優勢を維持することは不可能であると示すためには、同盟国軍は中国のものよりも分厚い非物理的効果の弾倉を持つ必要があろう。

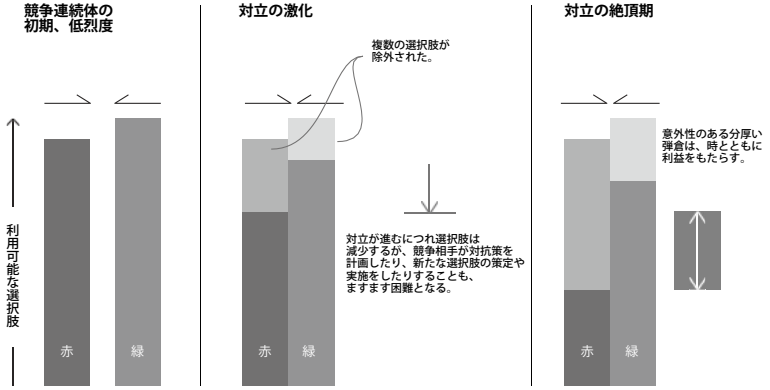


図 9：同盟国（緑）及び中国（赤）の非物理的能力の弾倉

米国はほぼ間違いなく世界で最も優れた非物理的効果のポートフォリオを展開している。また、米軍は各軍種において新たな一連の EW システムを配備しており、自衛を超えて、デコイの使用、欺瞞、スタンドイン（近距離）ジャミングのような攻勢的効果を実行し始めている。例えば、陸軍では地上レイヤーシステムを兵士、旅団、師団レベルで展開している[31]。海軍は SLQ-32 Surface EW Improvement Program system（艦載型電子戦能力向上プログラム）の改良版をミ

[31] Mark Pomerleau, “Army Pursuing New Electronic Warfare Architecture,” DefenseScoop, August 21, 2024, https://defensescoop.com/2024/08/21/army-pursuing-new-electronic-warfare-architecture/.

サイル駆逐艦（DDG）に装備しており[32]、空軍はスペクトラム戦航空団を新たな部隊や任務によって拡充している[33]。

米国政府は世界で最も優れたサイバーシステム及びEWシステムとオペレーターを有しているかもしれないが、一般に、戦時には部隊、艦艇、航空機の防護に、平時には特定の高度に特化された攻勢的な活動に焦点が置かれている。国防総省のサイバーツール、EW技術及びシステムのサプライチェーンには、長期にわたるセンシング及びセンスメイキング競争に関与するために必要な多様性及び能力が欠けている。米軍は、平時の諫止キャンペーンのために、戦時に優位に立つために必要な最も優れた「銀の弾丸」から、数年にわたり持続する競争において敵対者のセンシング及びセンスメイキングを弱体化させるために必要な「鉛の弾丸」又は「真鍮の弾丸」まで、多岐にわたる効果を必要とすると考えられる。

次に、米国及び同盟国の対センシング及び対センスメイキング・キャンペーンの概念について説明する。それに基づき、現在の及び今回提案する将来の非物理的なサプライチェーンの評価を行い、国防総省がEW及びサイバー効果開発の規模や速度をいかに改善できるかについて提言を行う。

3. 対センシング及び対センスメイキング・キャンペーンの実施

米国と同盟国の部隊は、キャンペーンの一環としてEW及びサイバー効果を最も効果的に使用できる。国防総省のサイバー戦略に記されているように、極秘の非物理的「銀の弾丸」を少数用意したとしても、抑止や諫止への貢献とはならな

---

[32] Sam LaGrone, “Navy Refining Plan for its $17B Destroyer Electronic Warfare Backfit with 4 Test Ships,” USNI News, January 19, 2024, https://news.usni.org/2024/01/19/navy-refining-plan-for-its-17b-destroyer-electronic-warfare-backfit-with-4-test-ships.

[33] Greg Hadley, “Spectrum Warfare Wing Adds Two New Squadrons to Handle Growing Mission,” *Air and Space Forces Magazine*, May 1, 2024, https://www.airandspaceforces.com/spectrum-warfare-wing-two-new-squadrons/.

い[34]。センシング及びセンスメイキングの観点からは、ごく少数の高度に洗練された非物理的ツールを戦時に使用することを計画している国防総省の指導者たちは、攻撃者がターゲティングの不備を数の力で克服するかもしれないというリスクを受け入れている。米軍と同盟国軍は、中国の近傍において PLA と対峙する可能性が高く、そこでは中国は軍需物資の量や補給において優位性があると考えられることから、この「銀の弾丸」アプローチが成功する可能性は低くなる。

国防総省のサイバー戦略は、非物理的能力をキャンペーンの一環として使用することを強調しているが、その主な関心は、米軍や公共インフラへの諜報や非物理的攻撃を妨害し、抑止することにある。米軍と同盟国軍は、マルチドメイン攻撃を抑止又は諫止しようとする場合には、サイバー空間や EMS にあるもののみならず、敵対者の作戦能力全般を劣化させる必要があろう。先に示したとおり、PLA の戦略と構想は、敵軍の位置と行動を把握し、長距離火器が照準するための偵察・情報システムの能力に依っている。そのため、米国の非物理的キャンペーンは、センシング及びセンスメイキングの競争に勝利することに焦点を当てるべきである。

同盟国軍が PLA のセンシング及びセンスメイキングを劣化させる経路は複数あるが、一つのアプローチは以下のとおりである。この例は、キャンペーンの一環として使用し得る能力や行動の種類を、秘密区分のないレベルで説明することを意図している。実際のキャンペーンはより複雑であり、秘密区分のある、かつ特化された様々な EW 及びサイバー効果を含むものになると考えられる。

センシング及びセンスメイキングにおける「オウンゴール」の回避

対センシング及び対センスメイキングの第 1 の原則は、「害をなさない」ことである。米軍と同盟国軍は、敵の偵察システムに対し、同盟国の欺瞞作戦を妨げるような、検知が容易な秘匿信号を提供することは避ける必要がある。例えば、モノ

---

[34] US DoD, *Summary of the 2023 Cyber Strategy of the U.S. Department of Defense* (Washington, DC: US DoD, 2023), https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

スタティックレーダーやデータリンクは、過去半世紀の間に対空監視、早期警戒、ミサイル防衛に不可欠となったが、プラットフォームの位置のみでなく、種類や秘密区分まで明らかにし得る。

主にモノスタティックレーダーやデータリンクの脆弱性により、冷戦中、米軍は電波輻射管制（EMCON）作戦を重視した。当然のことながら、ソ連崩壊後はEMCONの重要度は低下した[35]。しかし、近年、米軍はこのような慣行を作戦ルーティーンの一部として復活させた[36]。EMCONには主に、敵軍に探知される可能性がある際は、無線通信やレーダーの使用を最低限にすることが含まれている。しかしながら、パッシブRFとシグナルインテリジェンス（シギント）センサーは至る所に存在するため、同盟国軍は、低確度傍受／低確度探知（LPI/LPD）通信と組み合わせたパッシブ及びマルチスタティックなセンシングへとますます舵を切る必要があろう。

図10に示すとおり、同盟国軍はモノスタティックレーダーとは異なる複数種の新たなセンシング様式を追求することができる。近くの無人機に搭載した複数のRF受信機により、同盟国は、敵軍の無線通信又はレーダー輻射を探知し、敵軍の地理的情報を特定できる。無人航空機やミサイルがRFエネルギーで敵の艦艇や航空機を照射することにより、同盟国軍のプラットフォームはEMCONにとどまったまま、バイスタティックなターゲティングを行うことが可能になる。同盟国は、地域のテレビ塔や携帯電話基地局からのバックグラウンドエミッションを利用して、パッシブレーダーを用いた敵目標を照射できる。また、同盟国軍は赤外線捜索追尾システム（IRST）などのIRセンサーを使用して、敵部隊をその熱特性により発見、類別することができる[37]。

---

[35] Robert G. Angevine, “Hiding in Plain Sight—The U.S. Navy and Dispersed Operations under EMCON, 1956–1972,” Naval War College Review, Volume 64, Issue 2, 2011, https://digital-commons.usnwc.edu/nwc-review/vol64/iss2/6.

[36] Bryan Leese, “Living in TACSIT 1,” *USNI Proceedings*, February, 2017, https://www.usni.org/magazines/proceedings/2017/february/living-tacsit-1.

[37] US DoD, “Selected Acquisition Report (SAR): F/A-18 E/F IRST,” (Washington, DC: US DoD, 2023), https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Selected_Acquisition_Reports/FY_2022_SARS/IRST_SAR_DEC_2022_final.pdf.

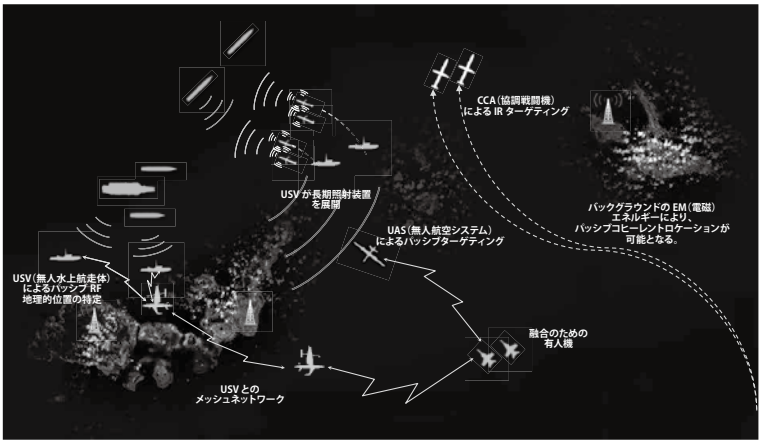


図 10：パッシブ及びマルチスタティックセンシングのコンセプト

パッシブ及びマルチスタティックセンシングは、通常、アクティブモノスタティックレーダーよりも探知距離が短く、精度に劣る。しかし、新興技術や技法は、同盟国軍がこのような欠点を緩和する一助となる[38]。例えば、消耗型無人システムを用いれば、敵部隊にかなり接近したり目標に照射したりすることで、有人の艦艇や航空機に比し低いリスクで敵軍の探知が可能となる。より高密度の RF 又は電気光学センサーは、レーダー、無線通信、又は赤外線放射に対し、より正確な方位を得ることができる。また、人工知能（AI）を用いて、人間による監視下で、実目標を用いた訓練をすることで、敵対者の目標の位置や類別の予測精度を向上させることができる[39]。

米軍と同盟国軍はまた、赤外線特性を減少させる必要がある。これは主にプ

[38] Jheng-Sian Li, Yung-Cheng Yao, Chun-Hung Chen, and Jyh-Horng Wen, “A Method to Improve the Accuracy of the TOA Position Location Solution in Multistatic Radar Systems,”Proceedings - 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2012, Pages 500-505, 10.1109/IMIS.2012.36.

[39] Denghui He, Yuanhui Cui, Fangchao Ming, and Weiping Wu, “Advancements in Passive Wireless Sensors, Materials, Devices, and Applications,” Sensors, Volume 23, Issue 19, 2023, Page 8200, https://doi.org/10.3390/s23198200.

ラットフォームの設計によりなされるが、偽装や熱源を追加することで、艦艇、航空機、車両の特性を不明瞭にし、敵の目標の類識別能力を低下させることができる[40]。こういったアプローチは、ロシアやウクライナの部隊が、現在行われている紛争において、敵のセンシング及びセンスメイキングに対抗するために利用している[41]。

シギント・センサーを欺く

対センシング及び対センスメイキング・キャンペーンは、デコイ作戦から始まると考えられる。敵のセンサーに対し多数の偽目標を作り出し、実目標からのリターンを曖昧にすることで、米軍と同盟国軍はPLAセンサーの信頼性を低下させることができ、ひいては、PLAの指導者たちがターゲティングと評価情報に依存している計画に対して抱く信頼もおとしめることができる。デコイは主に無人車両であり、そのため、上述のとおりパッシブ又はマルチスタティックセンシングネットワークの要素として、二つの機能を果たすことができる。

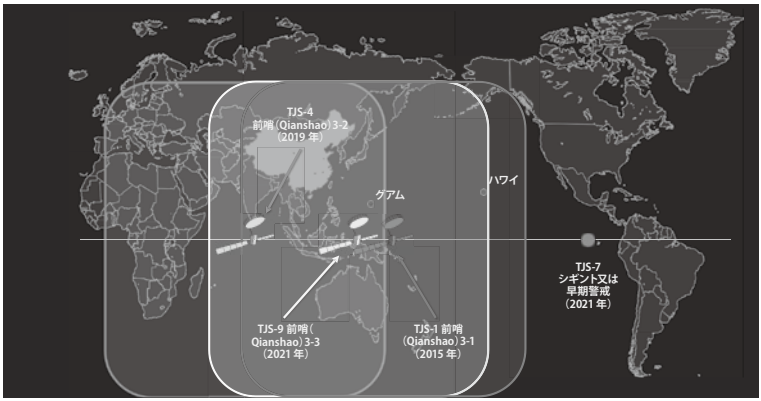
このキャンペーンは、図12に示すとおり、シギント衛星に対する作戦に重点を置く。これは、シギント衛星がPLAの偵察・情報システムの主要なセンサーと考えられる可能性が高いことによる。商用及び軍用シギント衛星は広範なエリアを見ることができるため、何百ものエミッターのおおよその場所を一度に特定し、周波数、パルス幅（PW）、パルス繰り返し周波数（PRF）、スキャンパターンなどの特徴を用いて、その類別を特定することができる。図11に示すような静止軌道（GEO）にあるシギント衛星は、一度に半球ほぼ全体を見ることができる。しか

---

[40] “Better camouflage is needed to hide from new electronic sensors,” *The Economist*, March 29, 2023, https://www.economist.com/science-and-technology/2023/03/29/better-camouflage-is-needed-to-hide-from-new-electronic-sensors.

[41] Dylan Malyasov, “Russia Uses Advanced Camouflage to Hide Their Iskanders from Ukrainian Drones,” Defense-Blog, April 19, 2022, https://defence-blog.com/russia-uses-advanced-camouflage-to-hide-their-iskanders-from-ukrainian-drones/; Sam Cranny-Evans, “The Role of Artillery in a War Between Russia and Ukraine,” *RUSI Commentary*, February 14, 2022, https://rusi.org/explore-our-research/publications/commentary/role-artillery-war-between-russia-and-ukraine.

し、GEO 衛星は方位線を 1 本しか受け取れず、また衛星が高高度にあるためエミッターのビーム幅が拡大することから、エミッターの位置を正確に特定することはできない。地球低軌道のシギント衛星は、エミッターに対し運動しており、かつ GEO 衛星よりも数が多いことから、複数の方位線を受け取ることができ、そのためより正確な位置情報を得ることができる。



注：本図に示す全てのコンステレーションは静止軌道にある。

図 11：PLA シギント衛星の覆域 [42]

米軍と同盟国軍は、EMCON の実践によりシギント・センサーによる探知可能性を大幅に減らすことができるが、無線通信やレーダー作戦が必要となることもある。艦艇、航空機及び陸上部隊は、限定的ではあるが必要な輻射が敵軍に対し実行可能なターゲティング情報を与えることがないよう、実際の部隊から離れた場所でデコイを使用することができる。デコイは、同盟国の必要な輻射によって映る実際の目標に代え、あるいはそれに加えて、評価と追跡の対象となる多数の目標を提供することにより、敵のセンシング及びセンスメイキングを混乱させること

[42] J. Michael Dahm, “Testimony before the U.S.-China Economic and Security Review Commission,” March 21, 2024, https://www.uscc.gov/sites/default/files/2024-03/J.Michael_Dahm_Testimony.pdf.

ができる。シギント・コンステレーションの視界に偽目標が存在すると知ると、オペレーターは全ての探知の調査を余儀なくされ、それによりセンスメイキングプロセスが遅れ、恐らく同盟国軍に主導権を渡すことになる。

本物のように見えるデコイには、実物のプラットフォームから放射される信号を少なくとも幾つかエミュレートできるRF送信機を組み込む必要がある。低コストのデコイは、海軍のSPY-1や陸軍のパトリオットのような大規模なレーダーを完全に表すのに十分な出力を有している可能性は低いが、RFデコイは独創的な方策や新しい技術を利用して、現実的なシミュレーションを提供することができる。例えば、探知を避けようとするレーダーオペレーターは、低出力でシステムを操作したり、又はスポットビームを利用したりすることがある。抗争環境下で使用されるデコイは、このような要求水準が低いモードのいずれかで運用されているSPY-1又はパトリオットを模することができると考えられる。

波形の生成は、RFデコイのもう一つの重要な課題である。汎用性を持たせるため、デコイは信号を生成する際にソフトウェア無線（SDR）を使用する必要があるかもしれない。SDRは、アンテナハードウェアの制限の中で、パルス繰り返し周波数、パルス幅、周波数といった様々な信号特性を生成するようプログラムすることができる。しかしながら、SDRにはかなりの処理能力も必要であり、どの程度SDRに汎用性を意図するかにより、必要な処理能力は増大する[43]。米軍と同盟国軍は、様々な無人システムに組み込むことが可能な、各々が狭い範囲の信号に特化したモジュール式の低コストかつ低出力のデコイ送信機を開発すべきである。

レーダーの出力と波形のエミュレーションは困難となり得るが、デコイはより簡単に実際の無線通信信号を作ることができる。無線機、特に地上部隊と車両が携行するものは小型で低出力であり、比較的低価格である。デコイのエミュレーターを作るよりも、米軍と同盟国軍は単に実際の無線機をデコイに組み込むべき

---

[43] Tore Ulversoy, “Software Defined Radio: Challenges and Opportunities,” *IEEE Communications Surveys and Tutorials*, Volume 12, Issue 4, 2010, Pages 531-550. 10.1109/SURV.2010.032910.00019.

であり、それにより敵のシギント・センサーに忠実度の高い欺瞞を提供できる[44]。装甲車やミサイル発射装置を模した無人車両を用いて、このアプローチを追求している企業も存在する[45]。

海軍もアクティブRFデコイを使用した実験を行っており、防衛関連企業は単なる自衛ではなく欺瞞のためのRFデコイシステムの開発・展開を開始している[46]。例えば、図12に示すように、Thales社は同社のHalcyon無人水上航走体（USV）にフランスのAccolade航空機搭載自己防衛デコイのEWペイロードを組み合わせた水上デコイの実演を行った[47]。

図12：デコイ実験で使用されたThales社Halcyon USV

大半の対シギント作戦はデコイに依存しているが、サイバー作戦により、シギント衛星コンステレーションの処理システムに偽目標を作ることもできる。商用シギント事業者に対しては、有線ネットワーク経由でこういったサイバー効果を持ち込むことができるが、軍用シギント衛星コンステレーションはインターネットのようなグローバル通信ネットワークからはファイアーウォールで守られている可能性が高

---

44 Walker Mills, “A Tool for Deception: The Urgent Need for EM Decoys,” US Military Academy, February 27, 2020, https://warroom.armywarcollege.edu/articles/tactical-decoys/.

45 Remy Hermez, “To Survive, Deceive: Decoys in Land Warfare,” War on the Rocks, April 22, 2021, https://warontherocks.com/2021/04/to-survive-deceive-decoys-in-land-warfare/.

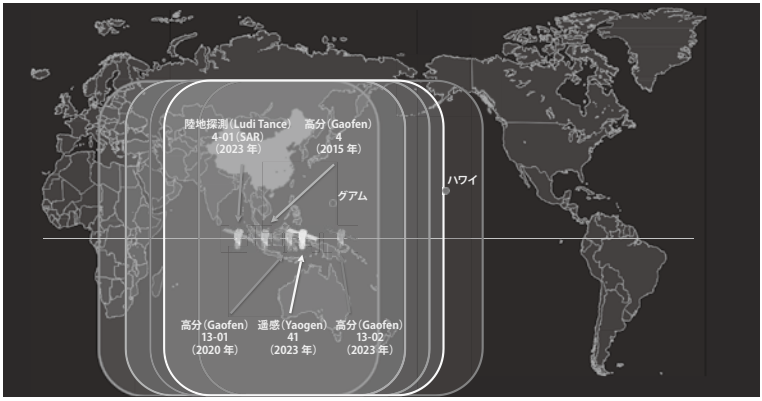
46 David Tremper, “Unmanned Sea Surface Vehicle Electronic Warfare,” *Naval Research Laboratory*, 2007, https://apps.dtic.mil/sti/tr/pdf/ADA518455.pdf.

47 Thomas Withington, “Winning Accolades,” Armada International, February 5, 2020, https://www.armadainternational.com/2020/02/winning-accolades/.

い。その結果、同盟国軍はシギント衛星自体のアンテナのような RF アパーチャ経由で、こうしたサイバーツールを挿入する必要が生じるであろう。

画像センサーへの対抗

多数の RF デコイに直面する可能性がある場合、PLA のオペレーターは、広範な地域をスキャンして忠実度の高い合成開口レーダー（SAR）リターンや可視光及び赤外線特性を取得できる画像衛星に目を向けるであろう。PLA の偵察・情報システムは、図 13 に示すとおり、電気光学・赤外線（EO/IR）画像衛星コンステレーションと SAR 画像衛星コンステレーションの双方を使用している。



注：「高分（Gaofen）」及び「遥感（Yaogen）」衛星コンステレーションは EO/IR センサーを使用し、「陸地探測（Ludi Tance）」は SAR センサーを使用している。本図に示すコンステレーションは全て静止軌道にある。

図 13：PLA の SAR 衛星及び EO/IR 衛星の覆域 [48]

EO/IR 及び SAR センサーには、各々、利点と欠点がある。SAR センサーはアクティブセンサーであるため、雲を透過でき、目標探知のために太陽光や熱源を

[48] J. Michael Dahm, “Testimony before the U.S.-China Economic and Security Review Commission,” March 21, 2024, https://www.uscc.gov/sites/default/files/2024-03/J.Michael_Dahm_Testimony.pdf.

必要としない。SAR センサーはまた、高解像度を達成するには大型かつ高価なセンサーを必要とする EO/IR 衛星に比し、武器ターゲティングの精度をより高めることができる[49]。しかし、SARセンサーは地表を斜めから見るためにレーダー画像が歪む可能性があり、EO/IR 衛星の方がより多様な目標の類識別を実現する可能性がある[50]。

SAR を欺く

対センシング及び対センスメイキング・キャンペーンにおける EO/IR と SAR 画像衛星の最も重要な相違点は、デコイとジャミングに対する脆弱性である。レーザーは可視光センサーや赤外線センサーを妨害できるが、これらはパッシブセンサーであることから、レーザーオペレーターはセンサーの存在とその正確な位置について他の情報源から把握しなければならないだろう。SAR 衛星は、その照射のために探知され、その位置を特定される可能性がある。また、他のレーダーのように、SAR 衛星はノイズジャミングで妨害されたり、異なる場所にある異なるプラットフォームをエミュレートした偽のリターンを提供するデコイに欺かれたりする可能性がある[51]。

SAR ジャマーは、デジタル信号処理を用いてレーダーリターンを操作できるため、エミュレートするシステムや車両よりも小型化できる[52]。図 14に示す対抗手段

---

[49] G. M. Koretsky, J. F. Nicoll, and M. S. Taylor, *A Tutorial on Electro-Optical/Infrared (EO/IR) Theory and Systems* (Alexandria, VA: Institute for Defense Analysis, 2013), https://www.ida.org/-/media/feature/publications/a/at/a-tutorial-on-e-lectro--opticalinfrared-eoir-theory-and-systems/ida-document-d-4642.ashx.

[50] Mark Ashby and Edmund Zelnio, “Multi-platform EO and SAR Fusion for Target ID,” *Proceedings of SPIE 12095: Algorithms for Synthetic Aperture Radar Imagery XXIX*, paper 1209505, May 31, 2022, https://doi.org/10.1117/12.2624109.

[51] Hua Li, Zhenning Li, Kaiyu Liu, Kaijiang Xu, Chao Luo, You Lv, and Yunkai Deng, “A Broadband Information Metasurface-Assisted Target Jamming System for Synthetic Aperture Radar” *Remote Sensing,* Volume 16, Issue 9, 2024, Page 1499, https://doi.org/10.3390/rs16091499.

[52] Dahai Dai, X. F. Wu, X. Wang, and Shunping Xiao, “SAR Active-Decoys Jamming Based on DRFM,” in *Proceedings of the IET International Conference on Radar Systems* (Edinburgh: IET, 2007), pp. 1-4.

の Leonardo AN/ALQ-260(V1) BriteCloud は消耗型デコイであり、これを組み込むことにより、防御対象の航空機に見えるようなリターンをレーダー誘導ミサイルに提供する[53]。スウェーデンの Saab 社は、近年、Gripen 戦闘機用に同様のデコイ試験を開始した。これには推進システムが組み込まれており、防御対象の航空機から脅威を遠ざけることができる[54]。また、図12に示したThales社のデコイ USV は、模擬対象の船舶のようなレーダーリターンを提供できるジャマーを搭載している。

出典：Leonardo社

図 14：防御対象の航空機を模す BriteCloud デコイ

上記に示したレーダーデコイの大半は、接近する兵器を防御対象のプラットフォームから遠ざけることを想定したものであるが、衛星レーダーや航空機搭載レーダーに対するデコイとして再利用ができる。このような対センシング及び対センスメイキング利用の場合、デコイが実際の米軍と同盟国軍に対する注意を引か

[53] Steven D'Urso, "A Deep Dive Into BriteCloud Advanced Expendable Active Decoy," The Aviationist, July 6, 2021, https://theaviationist.com/2021/07/06/a-deep-dive-into-britecloud/.

[54] Thomas Withington, "Decoy and Destroy," Armada International, October 7, 2020, https://www.armadainternational.com/2020/10/decoy-and-destroy/.

ないよう、防御対象のプラットフォームから離れたところで運用される必要があろう。

EO/IR を欺く

EO/IR 衛星は SAR センサーよりも欺くのが困難である。上述のとおり、防衛部隊は、EO/IR センサーに対し妨害あるいはデコイを使用するためには、同センサーが当該地域にあることを把握し、そのおおよその位置を知る必要がある。レーザーが利用できる場合には、防御対象のシステムの大きさにかかわらず、EO/IR センサーを妨害できる。EO/IR センサーを欺くためには、デコイがエミュレートしているシステムと同様の大きさと形状を有し、同程度の熱特性を有する必要がある。米国とそのアジアの同盟国は、冷戦後、デコイの広範な配備をほぼ停止したが、東欧の米同盟国はロシアによる攻撃の可能性を懸念し、デコイの研究開発と実証システムの配備を継続した。こういったデコイの大半は膨張式で、軽量かつ配備が容易である。多くはレーダー反射材を組み込んでおり、レーダー探知にも現れるようになっている。

図 15 に示すような膨張式のデコイは、チェコの Inflatech 社により製造されており、また、ウクライナ軍に対して供給されている可能性が高い。上空のセンサーに対し可視光及びレーダー特性を提供することに加え、図 15 に示すようなより新型の膨張式システムには、赤外線センサーを欺くため、エンジンや発電機からの熱を模すヒーターが組み込まれている。これらの特性は数百ヤード以上離れた距離では本物のように見え、ISR 航空機や衛星のセンサーに対して効果的なデコイとなる。

出典：Inflatech社

図 15：高機動ロケット砲システム（HiMARS）膨張式デコイ[55]

しかし、敵の無人航空機（UAV）は、本物のシステムと区別できるほど膨張式のデコイに接近できる可能性がある。例えば、膨張式のデコイは、たとえレーダー反射材が組み込まれていたとしても、レーダーが探知目標を類識別するために用いる固い反射面（hard edges）や、信憑性のある赤外線特性のためにヒーターを正確に配置する内部構造を欠いている。

デコイの開発者はデコイの忠実度を向上させており、同時に、大規模に配備し仮に喪失したとしても落胆しない程度に、デコイのコストと複雑さを低く抑えている。図16に示す組み立て中の木製レーダーのように、膨張式ではなく組立式のデコイは、その構造と動力発生においてより本物に近いデコイとなる[56]。米国陸軍は、近年、ジョージア工科大学の学生と組み、3日間の「ハッカソン」において、

---

[55] Associated Press, “Inflatable Tanks, Missiles: Czech Firm Makes Decoy Armaments,” March 6, 2023, https://apnews.com/article/czech-decoys-war-ukraine-russia-inflatable-a9c478adb9d7ecaa615cb19b25f4833f.

[56] Isabel Coles, “How Ukraine Tricks Russia Into Wasting Ammunition,” The Wall Street Journal, October 2, 2023, https://www.wsj.com/world/how-ukraine-tricks-russia-into-wasting-ammunition-799ed95f.

実用的な欺瞞システムを組み立てた[57]。

図 16：ウクライナの Metinvest 社におけるデコイレーダーの組み立て

実際のプラットフォームを効果的にエミュレートするには、デコイは、本物のシステムのように動き、防護される必要もある。そのため、機動性と擬装（カモフラージュ）という、実物の車両、艦艇、航空機を探知から守るために使用される手法を、デコイシステムにも用いる必要があろう。ウクライナ軍やロシア軍が配備している地上デコイの多くは、実際の移動式のシステムを模すために移動させることができるが、これにより移動を行う部隊にリスクが生じる。より実物に近づけつつ部隊へのリスクを減らすために、図 17に示すように、可視光及び赤外線デコイをけん引又は運搬できるか、あるいはそれ自体が敵の EO/IR センサーに対して本物のシステムをエミュレートできる無人車両を配備している企業が複数存在する[58]。

---

[57] "GTRI, Army Team Up for Decoy Hackathon," Georgia Tech Research Institute (GTRI), January 18, 2023, https://www.gtri.gatech.edu/newsroom/gtri-army-team-decoy-hackathon.

[58] Raider Targetry, "ATTLAS," https://raidertargetry.com/attlas-3/; Nick Reynolds, 'Heavy Armoured Forces in Future Combined Arms Warfare', *RUSI Occasional Papers*, 12 December 2023, https://www.rusi.org/explore-our-research/publications/occasional-papers/heavy-armoured-forces-future-combined-arms-warfare.

出典：Raider Targetry社

図 17：Raider Targetry 社の無人地上車両と細密な目標を組み合わせた可搬型移動目標システム（Mobile Moving Target System）

擬装は、単にデコイによる状況模倣の質を向上させる以上の利点をもたらす。実際のシステムとデコイシステムの双方を擬装することにより、両者の区別をより困難とすることが可能となり、忠実度が比較的低いデコイも効果を発揮できるようになる。多くの企業が、Saab 社の Barracuda シリーズ の擬装システムのように、複数の電磁スペクトラム領域にわたって作用する擬装を展開している[59]。

センサーフュージョンの拒否

米国と同盟国のデコイ及び欺瞞作戦は、完璧ではない。デコイは実際のプラットフォームの放射や動作を完全に表すわけではなく、また、軍隊にとり、艦艇や航空機のような大型プラットフォーム用の視覚的デコイや赤外線デコイを配備し操作するのは、困難を伴うであろう。その結果、米軍と同盟国軍は、PLA のオペレーターが AI アルゴリズムの支援を得て、複数種のセンサーからのインプットを用い、偽の目標と真の目標を見分けるというリスクに直面すると考えられる。この

[59] Saab, Barracuda MCS, Saab, https://www.saab.com/products/mcs-mobile-camouflage-system.

プロセスは、同一の目標に対し複数の検知が関連付けられる場合、センサー相関（sensor correlation）と呼ばれる。最新のデータ処理の到来により、現在、オペレーターは大抵の場合、複数のセンサーからのデータを組み合わせて単一の目標を作るセンサーフュージョンを追求している。センサー相関は、どのセンサーの探知目標が本物か偽物かを明らかにする一助となる。センサーフュージョンにより、防御側がジャミングや隠ぺいを試みたとしても、攻撃側は交戦に活用できる高品質のトラックを作り出せる可能性がある[60]。

PLAの偵察・情報システムは、恐らく、宇宙配備のセンサーからの目標トラックと中国本土に地上配備されたレーダーやパッシブRF受信機からの目標トラックとを、中国近くの領域外に配備された航空機センサーや船舶センサーからの補完を受けつつ、相関あるいは融合させようとするであろう。米軍と同盟国軍がシギント、SAR、EO/IR衛星に対して用いているデコイ、ジャマー、擬装は、陸上や航空機に配備された同様のセンサーに対しても効果的と考えられる。しかし、地上、艦艇、航空機センサーは、宇宙配備のセンサーとは異なる特性を有すると考えられ、米国と同盟国の部隊を、宇宙配備のセンサーとは別のより予測困難な角度から見る可能性が高い。これにより、効果のあるデコイ作戦やジャミング作戦を行うことは更に困難となろう。

一方で、センサーフュージョンは理論上は簡単に見えるが、実際上は困難である。データフォーマットやリフレッシュレート、検知に関連した特性は、センサーの種類によって大きく異なる。レイテンシーのレベルの相違により、複数のセンサーから同一の探知に関する報告がなされても、異なる目標に見える場合がある。また、配備されたセンサーからのデータはRF通信に依存しているが、これは環

[60] Joseph Peri, "Approaches to Multisensor Data Fusion," Johns Hopkins University Technical Digest, 2001, https://secwww.jhuapl.edu/techdigest/Content/techdigest/pdf/V22-N04/22-04-Peri.pdf/; Ashraf M. Aziz, "Fuzzy Track-to-track Association and Track Fusion Approach in Distributed Multisensor–multitarget Multiple-attribute Environment," *Signal Processing*, Volume 87, Issue 6, 2007, Pages 1474-1492, ISSN 0165-1684, https://doi.org/10.1016/j.sigpro.2007.01.001.

境条件やジャミング、電子欺瞞の影響下にある[61]。

同盟国軍は、センサーフュージョンが困難であることを利用して、複数のセンサーからのデータをリアルタイムで融合するPLAの偵察・情報システムの能力を妨害することができる。図18に示すように、デコイは偽のシギント、SAR、EO/IR目標を作り出す。空中早期警戒機（AEW）が調査に送られると、そのセンサーはジャマーにより不鮮明となり、その通信はEWシステムを搭載した小型UAVにより遮断される。SARジャマーは、実物の艦艇をSAR衛星の周波数域内におけるノイズの壁の背後に隠すことになると考えられる。

図18に示すデコイとジャミング作戦は、主に無人システムを用いて行われると考えられる。EMCONを適用している艦艇をエミュレートする場合、USVは、シギント衛星や陸上の傍受施設を欺くためには、低レベルの無線やレーダーの輻射のみで十分である。SAR衛星は長距離で作動しており、地球表面に到達するパワーはUSVから可能なレベル内である。また、USVに搭載され、AEW航空機や地上配備型短波（HF）レーダーのような地上のシステムに作用する無線やレーダージャマーは、目標とするシステムに更に接近することにより、出力の低さを補うことができる。

---

[61] S. Hamed Javadi and Alfonso Farina, “Radar Networks: A Review of Features and Challenges,” *Information Fusion*, Volume 61, 2020, Pages 48-55, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2020.03.005.

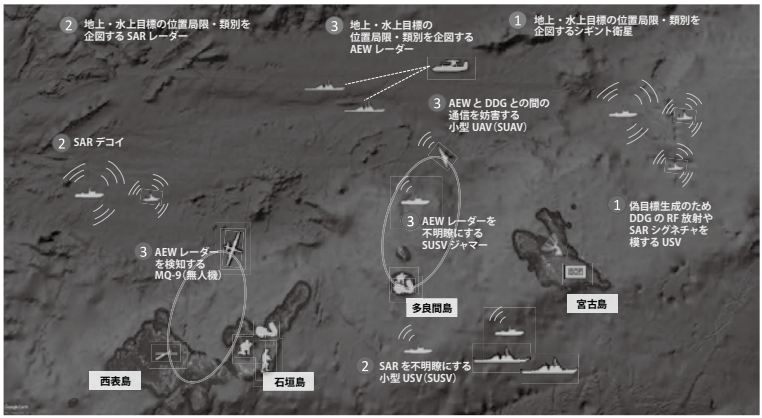


図 18：概念上の対センシング及び対センスメイキング・キャンペーンにおける努力の集中（lines of effort）

図 18 に示すようなジャマーは、敵のネットワークやシステムにサイバーツールを送り込むのにも役立つであろう。配備された航空機や艦艇は広域インターネットに接続されていないかもしれず、また、PLA は恐らく、ジャミングや阻止の影響を受けにくくするため、地上配備のレーダーやシギント・センサーを有線接続していると考えられる。しかしながら、それでもサイバーツールをシステムのアンテナに送り込む「フロントドア」攻撃に対しては依然として脆弱である。

中国のような大国に対しては、米軍と同盟国軍は、大量同時攻撃の競争で勝利する可能性は低い。軍隊とその指導者たちは、単に戦争発生時に勝利を願うのみでなく、紛争抑止に焦点を当てる必要がある。国防総省には、中国の攻撃を諫止するような平時の対センシング及び対センスメイキング・キャンペーンを維持するため、堅固な非物理的能力開発プロセスや産業基盤が必要となるであろう。

4. 結論

米軍はもはや、あらゆる敵対者に対しあらゆるシナリオを通じて、あまねく圧倒

的優位にあるとはいえない。中国のような同等の競争相手に対する優位を取り戻すには、米軍は対センシング及び対センスメイキング作戦にますます頼る必要があろう。こういった作戦は、戦時に敵軍の火力の有効性を軽減することに加え、敵対者の指揮官と指導者たちの、同盟国軍に正確に狙いを定め同盟国軍の将来の作戦を予測する自らの能力に対する信頼を損なわせることができる。

米軍と同盟国軍は、センシング及びセンスメイキングの競争において優位に立つには、相互運用性の向上、新たな拡散型低軌道（LEO）衛星コンステレーション、水上・水中・水域の上空における無人システムの継続的な進歩を通じて、自らのC3ISR能力を向上させる必要がある。更に重要なことに、同盟国軍は、敵対者が同盟国軍の作戦状況図を見たり把握したりする試みを挫くよう、大量かつ多様な非物理的サイバー効果及びEW効果を展開することも必要であろう。

国防総省の非物理的能力は、間違いなく最も優れている。しかし、米軍は野心的な要件を満たす比較的少数の優れた「銀の弾丸」効果を開発しているが、それが役立つのは、その使用が最大限の効果を発揮できる戦時のみである可能性がある。紛争を抑制するため、米軍と同盟国軍は、相手に対して相手のC3ISR能力が戦闘では信頼性に欠けるかもしれないということを示すために、平時の競争で使用できる非物理的能力が必要となろう。

非物理的手段を通じて攻撃を諫止する平時の努力を継続するためには、広範な損害や永続的な損害を与える可能性が低いサイバー効果やEW効果の分厚い弾倉が必要となろう。このような「真鍮」や「青銅」の弾丸は、相手側に与える損害がより大きいものに比べ、エスカレーションのリスクが低い。また、敵対者のシステムやネットワークにアクセスする難易度はより低いかもしれず、加えて一般的な攻撃方法を使用できると考えられることから、このような弾丸を大量に展開できる可能性が高い。

競争段階における非物理的効果もまた、たとえ通常はスタックスネット（Stuxnet）ウィルスのような攻撃やソーラーウィンズ（Solar Winds）ソフトウェアに対するサプライチェーン攻撃ほど劇的なものではなくとも、想定外のものである必

要があろう[62]。自己防衛ジャマーのような使用方法においては、予測可能な非物理的効果は望ましいが、対センシング及び対センスメイキングにおいては、相手に対しその C3ISR システムにより同盟国のサイバー攻撃及び EW 攻撃に対処できると示唆することになり、皮肉にも対戦相手を力づける方向へ作用する可能性がある。米軍と同盟国軍は、効果自体の新手のコーディングや波形、及び効果チェーン全体のデリバリーメカニズム、ターゲティングや戦術により、その非物理的能力に意外性をもたらし得る。

意外性をもった非物理的効果による分厚い弾倉を得るには、EW 及びサイバーサプライチェーンに対する異なるアプローチに加え、防衛産業基盤が必要であり、防衛産業が大規模に能力を構築し独自の革新を追求するインセンティブを与える必要があろう。本報告で提案するコンソーシアムとプロセスは、既存の取得及び契約権限を活用するものであり、政府が承認した情報やモデルを使用して産業界が新たなアプローチや効果を開発・評価するための「サンドボックス」となるだろう。政府は、最も有望な非物理的能力を競争価格で購入することにより、新たな効果への「けん引力」を生み出し、産業界主導の更なる革新を促すことになる。そのようなプロセスの一例は図 19 に示されている。

---

[62] National Public Radio, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," NPR.org, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack; David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, February 26, 2013, https://spectrum.ieee.org/the-real-story-of-stuxnet.

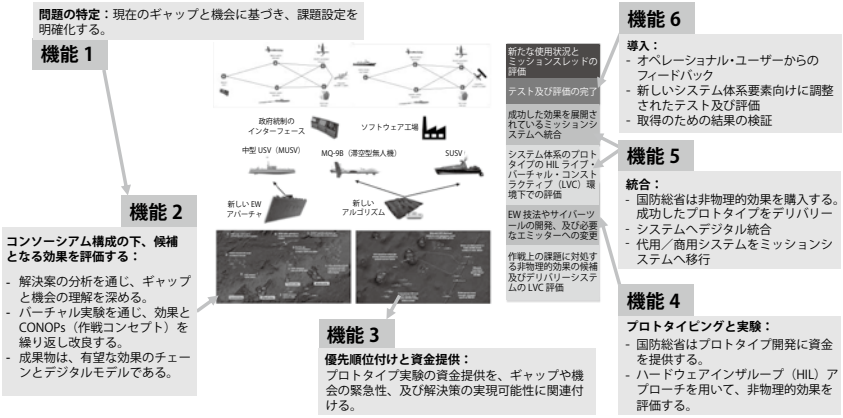


図 19：将来の非物理的能力開発プロセスの案

米国と同盟国の軍隊は、攻撃を抑止し打ち負かすために、もはや全般的な優勢に頼ることはできない。最近の複数の地域における事案を見れば、地域大国、国境を越えた組織、同等の競争相手の全てが、当該地域において、米軍と同盟国軍に圧力をかける能力や米軍と同盟国軍を上回る能力を得つつある状況が明らかである。非物理的効果により、国防総省が米国と同盟国が強みを持つ分野を利用して、対戦相手のセンシング及びセンスメイキングを弱体化させる取組を継続すれば、対戦相手を諫止する能力を回復する方法が得られる。しかし、このような強みを生かすためには、非物理的能力の購入と配備の方法を、物理的能力の購入と配備により近似させる必要があろう。