NPI

Nakasone Peace Institute

【報告書】

最終報告

台湾有事抑止のための対応要領及び多国間抑止態勢の構築―不可欠なハイブリッド戦対処

2026 年 3 月

海洋安全保障研究委員会

中曽根平和研究所
Nakasone Peace Institute

目　次

はじめに

１　本研究の概要

本研究委員会は、2023 年度から 2025 年度までの 3 年間、「台湾有事抑止のための対応要領及び多国間抑止態勢の構築」に関して研究を行った。

この研究に当たっては、「台湾有事」という用語に関する解釈を確定することが不可欠であるが、本研究委員会としては、これを中国による台湾への本格的軍事侵攻という狭い意味に解釈するのではなく、中国が軍事・非軍事を含む各種手段を複合させ、本格的軍事侵攻に至ることなく、いわゆるハイブリッド戦の手法によって強制的な統一に進むことも含めて広く解釈することとした。

その上で、台湾に対する中国の本格的軍事侵攻に関しては、これまでにも非軍事の要素も加味した研究やシミュレーションが数多く行われているのに対し、本格的軍事侵攻に至ることがないハイブリッド戦による台湾の強制統一に関しては、今まで十分な検討がなされてこなかったとの認識から、本研究では特にハイブリッド戦に焦点を当てて検討を行うこととした。

中国が台湾の強制的な統一を企図してハイブリッド戦の多様な各種手段を行使する際、その対象は台湾のみならず、日本、米国及びその他の関係諸国にも及ぶことが予測され、これに有効に対処するためには、多国間の連携が非常に重要であるとの認識の下、その具体的方向性についても検討した。

これらの具体的方策によって、中国による各種ハイブリッド戦手段の行使に有効に対処することができれば、本格的軍事侵攻未満の強制的統一を阻止することが可能であると同時に、中国がこれを諦め、本格的軍事侵攻に進もうとする際にも、中国が予め侵攻に有利な状況を作為するのを防ぐことが可能となり、トータルとして「台湾有事」の抑止に大きく寄与することになると考えられる。

２　2023 年度の研究

・「欧州ハイブリッド脅威対策センター」（The European Centre of Excellence for Countering Hybrid Threats: Hybrid CoE）のコンセプト・モデルを分析、本研究の指針を得た。
・本指針をもとに、台湾危機に関する独自のコンセプト・モデル構築のための前提として、本研究におけるハイブリッド戦を次のように定義した。
　ハイブリッド戦＝従来本格的軍事戦争で達せられてきた目的を、軍事・非軍事を含む各種手段によって、本格的軍事戦争に至らずに達成すること
・そのうえで、中国が本格的軍事戦争を生起させないようにグレーな状況で各種手段を組み合わせ台湾の統一を目指す場合を想定して、研究をすすめることとした。
・その一環として、欧州ハイブリッド脅威対策センター、欧州戦略コミュニケーションセンター及びフィンランド・ラトビア両国研究機関を訪問し、ハイブリッド戦関連の研究者と意見交換を行った。
・また、欧州ハイブリッド脅威対策センターのコンセプト・モデルで提示された 40 の手段

（Tool）をもとに、同手段を用いた予測される具体的活動及び過去の事例を抽出した事例集の作成に着手した。

3　2024 年度の研究

・中国は台湾の強制統一に向け、「懐柔路線」と「強硬路線」を巧妙に使い分けたハイブリッド戦を実施するとの前提の下に、事例集作成の過程で得られた「手段と活動」を基本として、想定モデルを作成した。
・この想定モデルの作成に当たっては、日本としての脆弱性を洗い出すため、個々のハイブリッド手段行使の蓋然性を追求するよりも、一連のシナリオの中で可能性がある手段を極力網羅した。
・この想定モデルを携えて、台湾の各種研究機関を訪問し、その妥当性について意見を聴取するとともに、現実に今台湾が直面している諸問題について意見交換し、台湾が抱えている脆弱性を考察する上での資を得た。
・その上で、本想定モデルに基づき、台湾を基点として、日本、米国、関連諸国に対して指向されるハイブリッド手段について改めて分析し、その際の日本の脆弱性を洗い出した上で、それぞれに対応する強靭性強化のための提言を案出した。

4　2025 年度の研究

・大きく世界の枠組の変化が想定される中、台湾強制統一を狙う中国のハイブリッド戦に関する想定モデルを踏まえ、本格的軍事侵攻による統一の企てとの関係を改めて整理・分析し、台湾有事抑止におけるハイブリッド戦対処の意義を洗い出した。
・24 年度の台湾訪問の成果等を踏まえ、改めてハイブリッド戦の分野で台湾が抱えている脆弱性を分析、また日本の強靭性強化策を踏まえ、中国が台湾に対して指向すると考えられる各種ハイブリッド手段を無効化するための有効な多国間連携の在り方について考察した。
・台湾、米国、オーストラリア、フィリピンの研究者と多国間連携の在り方について更なる意見交換を行うとともに、その成果を踏まえて他国研究者を含めたウェビナーを開催して討議を行うことを経て、最終的な提言を案出した。
・研究で使用したハイブリッド手段の事例集を更に充実させるとともに、研究から得られた予想事案も含めてデータベース化（英語版含む）し、今後各地で行われる研究に使用可能なようウェブ上で公開する予定である。

第１章　台湾有事抑止とハイブリッド戦対処

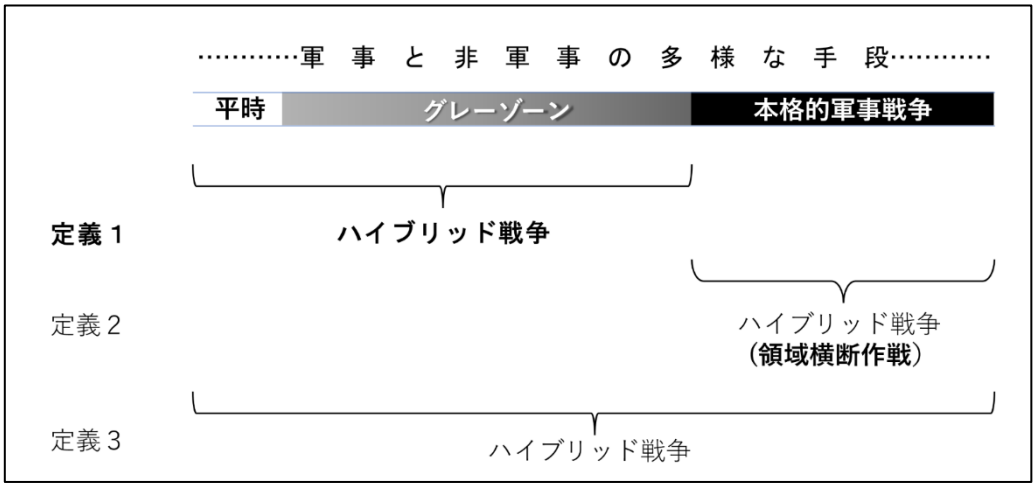
１　ハイブリッド戦の定義

近年、安全保障関連の論考においてハイブリッド戦という用語が多く使用されるようになってきたが、しかし論者によって、この用語が意味する内容は必ずしも同じではなく、この用語を用いて記述しようとする安全保障上の含意もそれぞれ異なる。そこで最初に本研究におけるハイブリッド戦の定義を明確にする。

育種学において２つの系統を掛け合わせるという語源から忠実に考えると、ハイブリッド戦と言う用語は、従来からある軍事的な戦争手段と、各種の非軍事的な手段を複合的に用いる戦争を指すと思われ、この点で多くの論者の考えは概ね一致している。

しかし論者によって大きく異なるのは、ハイブリッド戦を本格的軍事戦争との関係でどう位置付けるかである。ここで言う本格的軍事戦争とは、二つ以上の国家の正規軍の間で、それぞれの火力装備を駆使して戦われる烈度の高い戦争を指す。図１に示すように、本格的軍事戦争との関係でハイブリッド戦の定義は 3 つに分かれる。

図１　ハイブリッド戦の３つの定義



出典：松村五郎『ハイブリッド戦争の本質的メカニズム　－軍事・非軍事の諸手段を最終目的に結びつける「認知レベルでの戦い」－』2023 年、2 頁

最も広い定義は、この中の定義３であり、本格的軍事戦争に至らない平時やグレーゾーン事態における戦いから本格的軍事戦争における各種ハイブリッド手段の使用までを含んでいる。例えば、廣瀬陽子はその著書『ハイブリッド戦争－ロシアの新しい国家戦略』の中で、ハイブリッド戦争についてこのような広い意味でこの用語を使用している[1]。

これに対して定義２は、そもそも「戦争」という用語自体が烈度の高い武力紛争に関し

[1] 廣瀬陽子『ハイブリッド戦争－ロシアの新しい国家戦略』（講談社現代新書、2021 年）。

て用いられるものだという前提の下に、それ未満の事態でのハイブリッド手段の使用はハイブリッド戦の範疇には含めないというものである。また同様の観点から、ハイブリッド戦という枠組みで分析すること自体がミスリーディングであり、本格的軍事戦争の枠内で各種の新しい手段が用いられることに焦点を当て、領域横断作戦（全領域作戦または多領域作戦と呼称されることもある）という枠組みで考察すべきだとの論考も見られる[2]。戦争の本質が、今後も引き続き火力を中心とした武力行使にあるとの立場に立ち、新しい多様な手段が武力を最も効果的に発揮するために使用されると考えるならば、このアプローチは有効であろう。

それと反対に定義１は、本格的軍事戦争に至らない事態で、あるいは意図的に本格的軍事戦争に至ることを避けて目的を達成するために、軍事・非軍事の各種手段を用いることをハイブリッド戦と定義するものであり、多くの論者により使用されている[3]。今後、本格的軍事戦争がなくなるわけではないにしても、それに至らない新たな手法による戦いも重要になると考えるならば、本格的軍事戦争と明確に区別された定義 1 のハイブリッド戦という概念を導入した方が、議論が明確になる。

本研究においては、中国による本格的軍事侵攻に至らない台湾の強制統一に焦点を当てるため、ハイブリッド戦という用語を定義 1 の意味で用いることとし、「従来は本格的軍事戦争で達せられてきた目的を、軍事・非軍事を含む各種手段を複合させて本格的軍事戦争に至らずに達成すること」と定義する。

２　中国による台湾強制統一の４つのパターン

中国による台湾の強制統一の手法としては、本格的軍事侵攻によって、人民解放軍が台湾を物理的に占領するという方法の他に、ハイブリッド戦の手法によって、そのような大規模侵攻に至ることなく強制的に統一するという方法が考えられる。

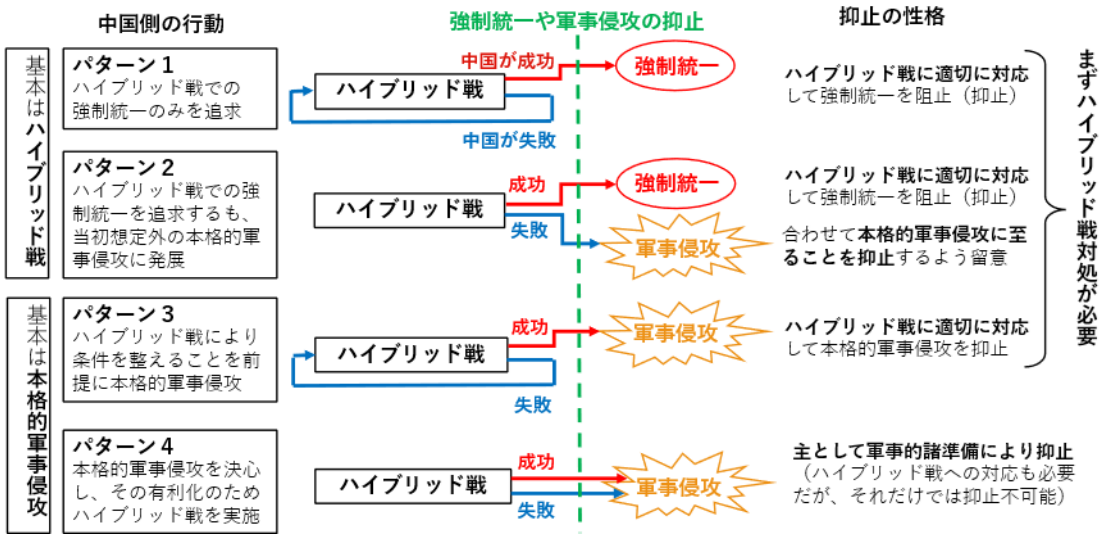
この際時系列的には、まずハイブリッド戦があり、場合によってはそこから本格的軍事侵攻に進むことになると考えられるが、この両者の関係には様々なバリエーションが考えられる。それを 4 つのパターンに整理してみたものが図 2 である。

---

[2] 渡部悦和、井上武、佐々木孝博『プーチンの「超限戦」－その全貌と失敗の本質』（ワニ・プラス、2022 年）、7～11 頁。

[3] 志田淳二郎『ハイブリッド戦争の時代－狙われる民主主義』（並木書房、2021 年）においては、多くの先行研究を参照した上で定義 1 の採用が妥当だとしている。11～62 頁。また、2017 年フィンランドのヘルシンキに、NATO、EU 及びそれらの加盟国によって共同で設立された欧州ハイブリッド脅威対策センターも、同様の認識の下で本格的軍事戦争に至らない事態におけるハイブリッド脅威への対処を主眼として活動している。“Hybrid threats as a concept”, The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)、https://www.hybridcoe.fi/hybrid-threats-as-a phenomenon/ (2023 年 9 月 13 日閲覧)。

図 2　中国による台湾強制統一の４つのパターン



出典：中曽根平和研究所海洋安全保障研究委員会 2024 年度報告書

中国側の行動方針は、ハイブリッド戦によって台湾を強制的に統一することを主眼とするのか、それとも本格的軍事侵攻によって占領することを主眼とするのか大きく 2 つに分けることが出来る。

その上で、前者の場合は、あくまでもハイブリッド戦を追求し本格的軍事侵攻は避けるパターン 1、ハイブリッド戦を追求しつつこれに失敗した場合に止むを得ず本格的軍事侵攻に移行せざるを得なくなるのがパターン 2 である。このパターンの危険性は、どちらの当事者も予期していないタイミングで本格的軍事戦争が生起するという点にある。

ハイブリッド戦を追求していたのに、その失敗で本格的軍事侵攻に移行せざるを得なくなるというのは奇妙に思われるかもしれないが、失敗に伴って内政上の危機が発生するのを回避すること、国際政治上自国が不利な立場に陥るのを避けること、あるいは大規模な軍事力で威嚇したにも関わらす功を奏さなかった際に今後威嚇の信ぴょう性が低下するのを避けることなどの理由が複合し、準備していなかった本格的軍事侵攻に移行せざるを得なくなる可能性はあると思われる。ロシアによるウクライナ侵略はこのパターンにあたると思われる。

これに対して当初から本格的軍事侵攻を念頭に置いて準備するのが、パターン 3 とパターン 4 である。準備の一環としてハイブリッド戦によって一定の条件を整え、それに成功した場合に限り本格的軍事侵攻に踏み切るのがパターン 3、ハイブリッド戦は行うが、その成否にかかわらずあくまで本格的軍事侵攻に進むことを予め決めているというのがパターン 4 である。

いずれの場合にも、台湾に対して政治、外交、経済、社会文化、情報、軍事など各分野での多様なハイブリッド手段が用いられるばかりでなく、日本や米国などにも、台湾強制統一を有利にするための各種ハイブリッド手段が行使されると考えられる。したがって、日本や米国が台湾と連携してこのような中国のハイブリッド戦に対する十分な対策をとる

ことによりこれを失敗に終わらせれば、パターン 1 による強制統一を阻止することができる。ところが、パターン２以下の場合には、これに加えて本格的軍事侵攻との関係という要素が絡んでくるため、分析はより複雑になる。

パターン２に対しては、ハイブリッド戦に対処すると同時に、その対処がうまくいっているが故に中国が本格的軍事侵攻に移行せざるを得なくなるという状況を防止しなくてはならない。すなわち、軍事侵攻に対する抑止力としての台湾及びこれを支援する側の軍事力強化も必要になる。またこれと合わせ、ハイブリッド戦の中で行われる大規模な軍事力による威嚇は、これが功を奏さない場合に本格的軍事侵攻に移行する可能性を秘めており、大規模な威嚇に指向しないような国際的な規範を強化することも重要である。

パターン 3 及びパターン 4 の二つのパターンは、分析を容易にするためにモデル的に両極端のケースを挙げたものであり、中国が軍事侵攻をする場合の実際の事態の推移は、この両パターンの中間になる可能性が高い。すなわち、ハイブリッド戦に失敗したら軍事侵攻しない、それでも断固軍事侵攻するという二択ではなく、中国がハイブリッド戦によって有利な条件の作為に成功するほど軍事侵攻を決心するハードルは低くなり、逆にそのような条件作為が阻止されるほどそのハードルは高くなると考えられる。すなわち、ハイブリッド戦に有効に対処するほど、軍事侵攻を抑止できる可能性が高まると考えてもよいだろう。

３　ハイブリッド戦対処の意義

前項で述べたように、中国によるハイブリッド戦に有効に対処してその企てを失敗に終わらせたからといって、それによって必ずしも本格的軍事侵攻を抑止できるというわけではないが、ハイブリッド戦への有効な対処は、軍事侵攻未満での強制統一を阻止することはもちろん、軍事侵攻の抑止や対処においても重要である。

その上で、各種手段を複合的に用いるハイブリッド戦自体を未然に抑止することは可能かどうかについて考えてみたい。一般論として、ハイブリッド戦において用いられる各種手段の一つ一つが行使される前に、それを未然に抑止することは非常に困難である。

その理由は大きく二つある。まず、ハイブリッド戦で使用される個別の手段は、平時から行使される非常に軽微な手段から攻撃的で烈度が高い手段までバリエーションが豊富であり、どの時点から行使され始めたのかを特定することが非常に難しい。

次に、ある特定の目的を達成するために各分野の手段が複合的に用いられるのが常であるが、当初は防衛側から見てそれらの統一的な目的や相互の関連性を看破することは困難であり、それが明確になった時には既にハイブリッド戦の渦中に巻き込まれているということになろう。

したがって、ハイブリッド戦の抑止を考える際には、あらゆる手段の行使を未然に防ぐということは現実的ではない。各分野においてそれ以上に事態が進展しないよう種々の対策を講じて、攻撃側が最終的に目的を達成する以前の、努めて初期の段階で諦めさせ、状況を安定化させるということになる。

この観点からは、日米台などが、それぞれ各分野での脆弱性を低減し、強靭性を高める施策を採ることが、中国のハイブリッド手段の有効性を減じることに繋がる。ハイブリッド戦が始まることを抑止することは不可能だが、一つ一つのハイブリッド手段の行使に対し、我の側の強靭性を高めることでその効果を減じるとともに、その都度相手にコストを付加してその継続をためらわせることで、相手側のハイブリッド戦による試みを中途で断念させることが重要である。

これらを総合して考えると、日米台などによるハイブリッド戦対処能力の強化は、
①中国のハイブリッド戦を、その都度無効化し状況を安定化させる
②中国がハイブリッド戦を続け、台湾を強制統一するのを阻止する
③中国が台湾に本格的に軍事侵攻するのを抑止する
④中国の本格的軍事侵攻が起きた際の有効な対処に資する
という 4 つの段階で、効果的な役割を果たすと考えられる。

4　世界情勢等が中国のハイブリッド戦に与える影響

当研究を開始したときからの世界情勢の変化、AI 等の技術の急速な進展、またパンデミック等が中国のハイブリッド戦へどの様な影響を与えているかは予断を許さないが、あえて概観を試みる。

(1) 米国と欧州の関係の不安定化等の影響

・中国にとって有利な状況の活用

中国は、ロシアによるウクライナ侵略及びそれへの対応等をめぐり米国と欧州等の各国の関係が不安定化し国際秩序が動揺している状況を利用し、台湾と米国の関係を弱体化させるためのハイブリッド戦を展開するであろう。今後、中国はこのような状況を最大限に利用し台湾の米国に対する不信感を増大させるためのハイブリッド戦を実施し、自国に有利な状況を作り出そうとすると考えられる。特に、2025 年 1 月に「米国第一主義」を掲げる第 2 次トランプ政権が発足したことから、中国が米国と同盟国・パートナー間の関係を離反させる好機とみなし、米国と台湾、日本その他の同盟国・パートナー国との関係の弱体化、相互の不信感の増大等を企図したハイブリッド戦を実施する可能性が増大するであろう。

・経済的、軍事的関係の再構築

米中の経済的対立が続く中で、中国は他の国々との経済的・軍事的な関係を強化し、米国の影響力を削ぐであろう。例えば、中央アジア、東南アジア諸国やアフリカ諸国との協力、そして欧州との関係の再構築をはかり、米国を国際的に孤立させようとするであろう。結果いわゆる「戦狼外交」といった強硬な外交姿勢は当面影をひそめるかもしれない。

・サプライ・チェーンの再編

米中間の経済的な対立が続く中で、中国はサプライ・チェーンの多様化を進め、米国優位のドル決裁圏とは別の、自国に都合の良い国際経済関係を構築しようとするであろう。

・技術の自立と非対称戦能力強化

米国が中国に対して課している関税や輸出規制は、中国の経済成長や技術開発に影響を与え、これにより、中国は国内の技術的自立を加速させる一方で、サイバー攻撃や情報操作といった非対称的な手段を一層強化するであろう。

・米国の政策批判のプロパガンダ

米国の政策を批判するプロパガンダを国内外で展開しその活動を強化し、国民の愛国心を高めるとともに、グローバル・サウス諸国の支持を得ようとするであろう。

・「米国は台湾を見捨てるかもしれない」との情報発信

中国は、欧州諸国に対して米国の信頼性を疑問視するような情報を流し、米国との関係を再考させるよう誘導する。また、台湾国内でも「米国は台湾を見捨てるかもしれない」といった不信感を醸成するための情報を発信し、これらの情報の信ぴょう性が高いと認識させることを企図したハイブリッド戦を展開する可能性がある。

・米国の台湾への軍事支援の低下を作為

台湾周辺で軍事演習を繰り返し、台湾の安全保障に対する米国の関与を試す可能性がある。長期的には米国が同盟国により多くの防衛上の負担を分担させて、自身は大国間のパワーバランス維持に注力するようになる中で、米国から台湾への軍事支援が減少する状況を作り出そうとする可能性がある。

(2) 北朝鮮、ロシアは台湾統一にどのように影響するか

中国、ロシア、北朝鮮は急速にその蜜月ぶりを演出している、果たしてこれが本物なのかは不明である。例えば中国が台湾統一への軍事力の行使に移行した場合に、果たしてロシア、北朝鮮がどの様に軍事的に関与するのか、その国力から軍事的な支援は避けたいというのが両者の本音なのではないか。その前提にたてば、ロシア、北朝鮮は中国のハイブリッド戦を間接的に支援し、中国との関係を維持したいと考えるのではないか。今後はハイブリッド戦の中でも、重要な部分を占めると思われるサイバー攻撃、あるいはインフラ攻撃に関して中国、ロシア、北朝鮮の 3 者が連携する可能性を考慮しておく必要がある。

(3)ロシアによるウクライナ侵略の影響

・ミサイル、核の威嚇によるゆさぶりをかける可能性

中国はウクライナ侵略に際しロシアが実施した核兵器による威嚇から得られた教訓を利用するであろう。

・ロシアのハイブリッド戦のノウハウを導入

中国のハイブリッド戦能力はロシアよりも 5 年程度遅れているといわれているが、急速にキャッチアップしていると思われる[4]。

[4] 防衛研究所、https://www.nids.mod.go.jp/。

(4) 生成 AI 技術の急速な進展

中国の生成 AI 技術は急速に発展しており、特に生成 AI を用いて作成されたディープフェイクの精度は向上している。中国はこれらの技術を用いてその真偽の判別が困難な戦略的ナラティブを SNS や動画プラットフォームで拡散している。また悪意を持った攻撃者による大規模言語モデル（LLM）の学習データの汚染は相手の国の世論に大きな影響を与えるハイブリッド戦の新たな手段として注意を要する。

(5) コロナパンデミックの影響

パンデミックは、中国のハイブリッド戦の手法をさらに多様化させる契機となったと思われる。

・ウイルスの起源や対応に関する国際的な批判に対抗するため、プロパガンダや世論操作について経験を積んだと思われる。
・リモートワークやオンライン活動の増加に伴い、サイバー攻撃、サイバー空間上での情報搾取の重要性を更に認識した。
・医療物資の供給を通じて外交的な影響力を行使できることを学んだと思われる。

第２章　欧州ハイブリッド脅威対策センターのコンセプト・モデルの分析

2014 年のクリミア危機において、ロシアは正規軍による軍事侵攻に先立ち、通信網の遮断、フェイクニュースの流布、SNS を用いた世論操作等の非正規の手段を駆使し、ほぼ無血でクリミアを占領し「併合」した。2022 年 2 月に開始されたロシアによるウクライナ侵略に際しても、同様の展開が予測されていた。しかし、ロシアによるハイブリッド戦は成功せず、結果として軍事侵攻へと発展した。この 2014 年と 2022 年の違いを生んだ要因の一つとして注目されるのが、「ハイブリッド脅威のコンセプト・モデル」（以後、「コンセプト・モデル」とする）に基づく対策である。

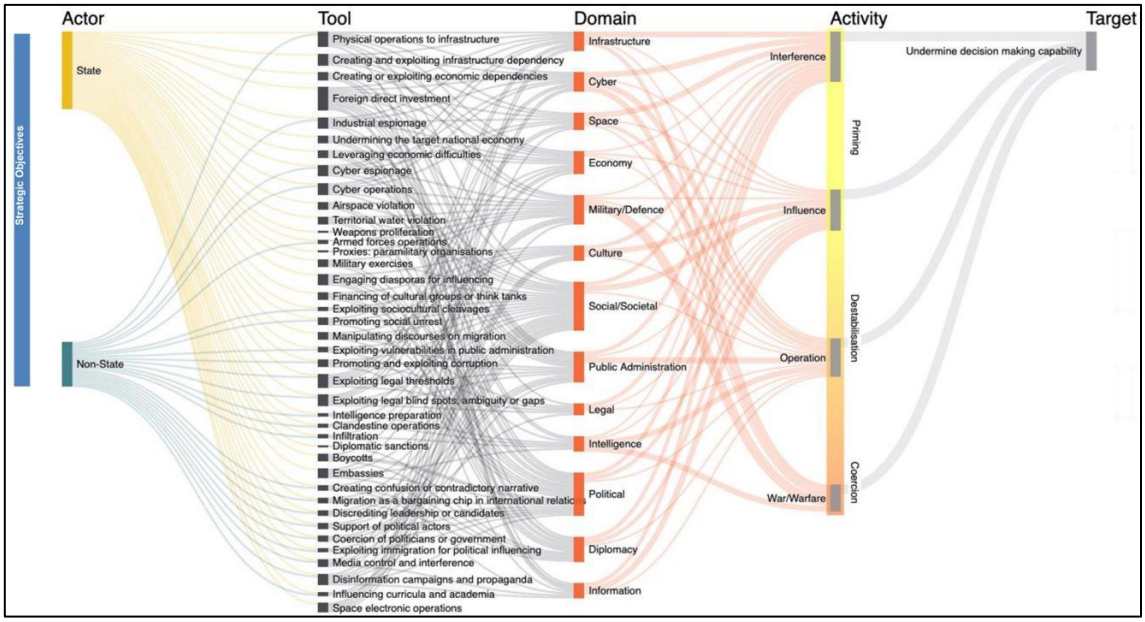
このコンセプト・モデルは、欧州ハイブリッド脅威対策センターが欧州委員会の共同研究センターの協力を得て、2018 年 7 月から約 2 年間をかけて作成したものであり、ロシアによる侵攻において生起した諸事象を体系的に理解するために活用されたと考えられる。

本研究では、このコンセプト・モデルを参考にしながら研究を進めたが、まずはその概要と基本的な考え方について分析を行う[5]。

１　コンセプト・モデルの全体像

ハイブリッド脅威のコンセプト・モデルの全体像（図 3）は以下のとおりである。

図 3　ハイブリッド脅威のコンセプト・モデルの全体像



出典：**European Commission, & Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, 2021, p. 13**

[5] 川嶋隆志「ハイブリッド脅威分析のフレームワーク―欧州ハイブリッド脅威対策センターのコンセプト・モデルを通じて―」NPI コメンタリー、2022 年。

このコンセプト・モデルの分析フレームワークは、以下の４つの柱から構成されている。

(1) アクター
(2) ツール
(3) ドメイン
(4) アクティビティ

以下では、それぞれの要素について概説する。

２　コンセプト・モデルのフレームワーク

(1) アクター

アクターは、国家主体と非国家主体の２種類に分類される。国家主体とは、EU、NATO など民主主義国家を構成する勢力に敵対する権威主義国家を主に指す。これらの国家の特徴として、政権の目的が権力の維持にあり、民主主義国家に対して恐れを抱いている傾向が見られる[6]。具体例としては、ロシア、中国、イラン、北朝鮮が挙げられ、特にロシア及び中国はハイブリッド脅威の主要なアクターとされている[7]。

一方、非国家主体とは、国家の正式な機関に属さずとも国際関係に関与し、干渉・影響・変化をもたらすだけの力を有する実体を指す。国家が非国家主体を通じて他国に対して有害な活動を行うケースも多く見られる[8]。代表例として、ヒズボラ、ISIL、民間軍事会社（PMC）などが挙げられる[9]。ハイブリッド脅威への対応においては、これらの国家主体・非国家主体の特定に加え、アクターの戦略目的を分析することが重要である[10]。

(2) ツール

ツールとは、国家主体および非国家主体がハイブリッド脅威を対象に及ぼすために用いる手段をいう[11]。本コンセプト・モデルでは、過去の事例に基づき 40 種類のツールが提示されており、アクターはこれらを組み合わせて、ハイブリッド脅威を構成する。

(3) ドメイン

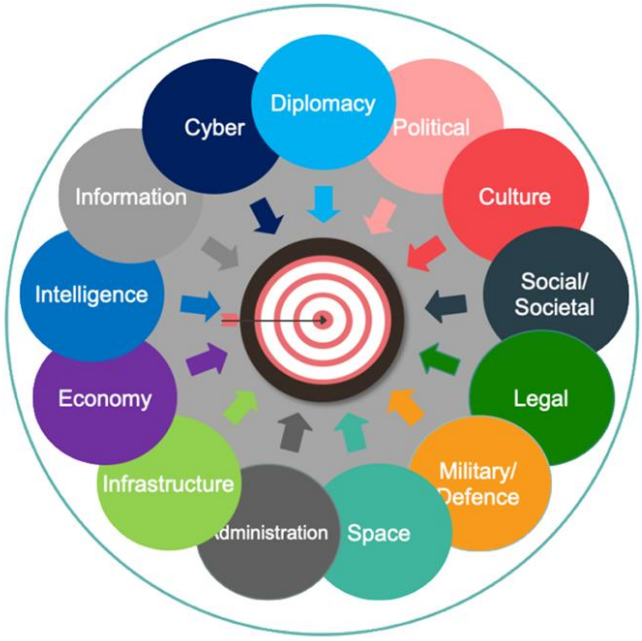
ドメインは日本では安全保障の文脈で「領域」とも呼ばれるが、ここでは国力の要素をグループ化したものであり、アクターがツールを利用してハイブリッド脅威を及ぼす標的となる[12]。アクターは、ドメインを標的とすることで、最終的な戦略目標の達成を図る。図 4 に示されるように、軍／防衛のほか、インフラ、サイバーなど、政治、経済、社会を構成

---

[6] European Commission, & Hybrid CoE, The Landscape of Hybrid Threats: A Conceptual Model Public Version, 2021, pp. 16-18, https://www.hybridcoe.fi/wp content/uploads/2021/02/conceptual_framework reference-version-shortened good_cover_-_publication_office.pdf (2022 年 5 月 1 日閲覧)。
[7] Ibid., p. 16.
[8] Ibid., p. 22.
[9] Ibid., p. 16.
[10] Ibid., p. 15.
[11] Ibid., p. 33.
[12] Ibid., p. 26.

する 13 の要素がドメインとして列挙されている。アクターは、各ドメインに属する複数のツールを組み合わせて、図の中央に示された目標の達成を試みる。

図 4　ドメインとアクターの目標のイメージ図



出典：European Commission, & Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, 2021, p. 27

なお、本コンセプト・モデルでは、ドメインの分類に理論的根拠に基づいた厳密なグループ化は行われておらず、ケースに応じた変更・見直しが必要とされている[13]。

●ハイブリッド脅威活動のツールと影響を受けるドメイン

敵対するアクターが目的達成のために使用可能なツールと影響を受ける可能性のあるドメインについては別紙１に整理した。

アクターはツールを用いて１つ以上のドメインに影響を及ぼすほか、ドメインの脆弱性を標的とすることもある。また、直接的な影響に加え、他のドメインへ波及する「カスケード効果」をもたらす場合もある[14]。

別紙１において注意すべき点は、ツールの使用兆候が見られたからといって、それが直ちにハイブリッド脅威であるとは限らないことである。例えば、サイバー・オペレーションは、他のツールと連動してハイブリッド脅威の一部として行われる場合もあれば、単独で実施される場合がある[15]。あるハッカーによるサイバー攻撃が発生した際には、戦略目的

[13] Ibid., pp. 26-27.
[14] Ibid., pp. 11-12.
[15] Ibid., pp. 32-33.

を持つアクターとの関連性や、他のツールとの連動性を分析し、それらが組み合わさった結果として生じる影響の全体像を早期に予測する必要がある。

(4) フェーズとアクティビティの関係

ツールを用いたアクティビティは、以下の３つのフェーズによって強度が異なる[16]。本研究会では、各フェーズとアクティビティの関係を別紙 2 に整理した。

別紙 2 におけるフェーズとアクティビティの関係は、完全に固定的なものではない。条件形成フェーズでは主として撹乱、一部影響行使という形で、不安定フェーズでは主として影響行使、一部作戦実施という形で、強制フェーズにおいては主として作戦実施という形で、各ツールを使用した各アクティビティを組み合わせ、各フェーズに応じたハイブリッド戦を構成していくものと考えられる。以下各フェーズの詳細を説明する。

- 条件形成フェーズ[17]

このフェーズでは、アクターが対象国に対して各種ツールを用いたアクティビティにより「撹乱」を行う。対象国が状況認識を失い、政府首脳部がアクターに有利な意思決定を自発的に行うよう誘導することがアクターの最終目標である[18]。「撹乱」の次に来るアクティビティが「影響行使」である[19]。このフェーズにおける活動は曖昧で目立ちにくく、ハイブリッド脅威として即座に評価することが難しい。

- 不安定化フェーズ[20]

このフェーズでは、アクターが各ドメインにおいて、ツールを用いたアクティビティを強化する。活動は顕在化し、攻撃性を増し、物理的な打撃や暴力を伴うことが多くなるが、アクター自身の関与は秘匿される傾向がある。

例えば、武力衝突が発生し、死者数の報道、遺族や負傷した兵士のコメントなどが拡散される（撹乱）。その後、死者数増加の報道、遺族のコメント等が増えていくと、兵士の家族の不安が高まる（影響行使）。さらに社会全体に不安が波及し、政府への不信感が高まり、デモ等の扇動が行われるようになる。不安定化フェーズにおけるアクターの目標は、対象国を揺るがし、容易に屈服させられるレベルまで不安定化させることである。所要の効果が得られない場合には、再び条件形成フェーズに戻り、より効果的なツールの組み合わせに変更することもある。

- 強制フェーズ[21]

このフェーズでは、政治的・経済的措置、破壊、情報、偽情報拡散及びプロパガンダ活動、特殊部隊の隠密行動、対象国の敵対勢力への軍事支援が行われ、対象国に対して戦略目的を強制的に達成しようとする。

すべてのドメインがハイブリッド脅威の対象となり、テロ、妨害、転覆、ゲリラ戦争等

---

16 Ibid., p. 10.
17 Ibid., pp. 37-40.
18 Ibid., p. 37.
19 Ibid., p. 38.
20 Ibid., pp. 40-41.
21 Ibid., pp. 41-42.

の限定的な軍事的手段も使用される。さらに、軍事戦争が本格的に開始される場合には、各ツールが、軍事戦争を有利に進めるために活用されることもある。

ここでは強制フェーズにおける戦争もアクティビティの一部として記載しているが、こうした本格的戦争におけるツールの使用は、軍事戦争の一部としての領域横断作戦と位置付け、本研究の対象外とした。

第３章　ハイブリッド戦の手段と事例の分析

本章では前章で示した敵対するアクターが目的を達成するために使用可能な 40 のツールをもとに、工作手段となり得る事例を公開情報から収集し、分類・分析を行う。

１　工作手段の概要と具体例

ツールは、インフラ、経済、サイバー、軍事、文化、社会、行政、法律、インテリジェンス、外交、政治、インフォメーション、技術の 13 の工作手段のグループに分類される。

13 の工作手段の概要は別紙 3 に示し、以下に具体例を紹介する。

(1) インフラに関連した工作手段

インフラは国民生活や経済活動の基盤であるため、影響工作を受けると、インフラの機能が停止または低下し、社会に大きな混乱をもたらす。特にハイブリッド戦においては、「インフラに関連した工作手段」が SNS やメディアを通じた偽情報の拡散など、他の工作手段と組み合わさることで、国民の不安を煽り、対象インフラへの影響にとどまらず、経済や社会など多方面に波及する効果を持つ。

●「インフラに対する物理的打撃」の例

2023 年 2 月に台湾馬祖列島の海底ケーブルが切断された際には、電話だけでなく、ネットバンキング、航空機予約などにも支障が生じた。台湾では過去 5 年間で 20 回を超える海底ケーブルの切断事象が報告されている[22]。

海底ケーブルは通信だけでなく、経済、金融、国家の安全保障に至るまで広範な役割を担っている。世界には約 500 本、総延長 150 万 km（地球約 37 周分）に及ぶ主要ケーブルが張り巡らされている[23]。

この海底ケーブルの切断は、目撃者のいない海洋で行われることが多く、切断した船舶の特定が困難である。仮に特定できたとしても、事故を装っていた場合には故意性の証明が難しく、公海上での切断であれば国際法上の取り締まりも困難である。

なお、日本と接続する海底ケーブルは約 30 本存在し、1～2 本切断しただけでは大きな影響はないとされるが[24]、海底ケーブルの陸揚げ地点が特定地域に集中しているため、その脆弱性が課題となっている。

●「インフラへの依存の構築と利用」の例

2014 年のロシアによるクリミア併合後、ウクライナの通信会社はクリミア半島から撤退

---

[22] 読売新聞オンライン「海底ケーブル切断で電話やネット遮断、中国船関与か…台湾本島で同様の事態懸念」、2023 年 3 月 2 日、https://www.yomiuri.co.jp/world/20230302-OYT1T50368/（2025 年 9 月 19 日閲覧）。

[23] METI Journal online「“データの大動脈”海底ケーブル 日本への「信頼」テコに世界シェア拡大目指す」、2023 年 12 月 25 日、https://journal.meti.go.jp/p/40663/（2025 年 9 月 19 日閲覧）。

[24] NHK「知られざる海底ケーブルの世界」、2023 年 6 月 20 日、https://www3.nhk.or.jp/news/html/20230620/k10014104331000.html（2025 年 9 月 19 日閲覧）。

し、2017 年にはウクライナ政府が同地域へのインターネット接続サービスの提供を停止した。

一方、ロシアの国営通信会社ロステレコムは、ロシア本土とクリミア半島を結ぶ通信ケーブルを敷設し、クリミア半島のインターネット接続をロシア経由に切り替えた。これにより、クリミアの住民はロステレコムを通じてインターネットを利用することとなり、ロシア当局による検閲や監視の対象となった[25]。

(2) 経済に関連した工作手段

「経済に関連した工作手段」は、相手国の経済に働きかけることで、国家の意思決定や社会機能に重大な影響を与える手段である。特にハイブリッド戦においては、「フェイクニュースや SNS を通じた情報操作と組み合わせることで、国民の不満や政府への不信感を煽る効果があり、ハイブリッド戦の極めて重要な手段の一つである。

●「経済に関連した工作手段」の例

2022 年のロシアによるウクライナ侵略の際、欧州の天然ガス消費量の約３分の１がロシアからの輸入に依存しており、その大部分はロシアと欧州を結ぶパイプラインによって供給されていた[26]。この状況は対ロシア制裁との関係で大きな問題となった[27]。

同年 9 月、ロシアはパイプラインの修理を理由に「ノルド・ストリーム１」を経由する欧州へのガス供給を完全に停止した。ロシアは欧州向けのガス輸出量を大幅に削減しており、西側諸国はロシアがエネルギー供給を戦争の武器として利用していると批判したが、ロシア側はこれを否定している[28]。

2025 年現在、EU はロシア産エネルギーへの過度な依存を安全保障上の脅威と位置付け、ロシア産エネルギーからの完全脱却に向けた取り組みを進めている[29]。

(3) サイバーに関連した工作手段

「サイバーに関連した工作手段」には、活動主体が国家なのか非国家主体なのかを特定しにくいという特徴がある。国家関与を否定しやすく、また隠密性が高いため、いつから工作活動が始まっていたのかを把握することも困難である。

特にハイブリッド戦においては、サイバー攻撃によって通信を妨害し、その混乱を利用して軍事行動を展開するなど、経済、情報、軍事など他の工作手段と連動した複合攻撃に

---

25 朝日新聞 GLOBE＋「ウクライナからロシアに切り替えられたネット接続　クリミア半島の異変、日本から観測」、2022 年 7 月 17 日、https://globe.asahi.com/article/14669860（2025 年 9 月 19 日閲覧）。

26 日本経済新聞「ロシア―欧州間パイプラインとは　独、消費量の大半依存」2022 年 2 月 8 日、https://www.nikkei.com/article/DGXZQOUB0860Q0Y2A200C2000000/（2025 年 9 月 19 日閲覧）。

27 原田大輔「対露制裁の現状と見通し」日本国際問題研究所、8-15 頁、2022 年 10 月 14 日、https://www.jiia.or.jp/topic-cdast/event/20221014-01.pdf（2025 年 9 月 19 日閲覧）。

28 BBC News Japan「ロシアのガス大手、欧州への供給を 3 日間停止 修理のためと」https://www.bbc.com/japanese/62747358（2025 年 9 月 19 日閲覧）。

29 ジェトロ「欧州委、ロシア産エネルギーからの完全脱却計画を発表、2027 年末までにガス輸入禁止へ」、2025 年 5 月 9 日、https://www.jetro.go.jp/biznews/2025/05/1e677dd0cec3e0c2.html（2025 年 9 月 19 日閲覧）。

活用されることが多い。

●「サイバーに関連した工作手段」の例

2022 年のロシアによるウクライナ侵略の際、ロシアは侵略以前からウクライナ国内の政府機関、軍、メディア、重要インフラに対してサイバー攻撃を行っていた。これらのサイバー攻撃はインフラ設備の妨害や、外交・軍事情報の秘密裏な入手を目的としていたとされる。しかし、ウクライナ政府やマイクロソフト社などが事前に対策を行っていた結果、大規模な被害につながらなかったと報告されている[30]。

(4) 軍事に関連した工作手段

軍事演習、領空・領海侵犯などは、相手国に対して自国の軍事力を誇示することで、国民や政府に心理的圧力をかける手段として用いられる。特に国境付近や係争地域での演習や軍の展開は、相手国の不安を煽り、外交交渉における優位性を確保する目的で実施されることがある。

特にハイブリッド戦においては、サイバー攻撃によって情報システムを麻痺させ、軍の指揮系統や通信を混乱させた後に軍事力を展開する、軍事演習と同時にプロパガンダや偽情報を用いて相手国の世論を操作し、政府への不信感を煽る、あるいは国際法の曖昧性を利用して軍事行動を正当化するなど、サイバー、インフォメーション、法律と複合的に組み合わせることで、工作の効果を増大させることが可能である。

●「軍事に関連した工作手段」の例

2024 年 5 月 23～24 日、中国は台湾周辺海域において軍事演習を実施した。この演習では、実際には行われていない実弾攻撃をリアルなコンピューター・グラフィックで演出したほか[31]、中国系メディアが「台湾空軍の若手パイロットが疲労で退職を希望している」と報道するなど[32]、台湾住民の不安を煽る情報操作が行われた。これらの手法は、台湾社会に対して心理的圧力を加えることで、台湾の有権者の間に戦争への懸念を広げ、民進党政権への支持を低下させることを通じて、台湾の統治の安定性と防衛意志を揺るがすことを目的としている[33]。

(5) 文化に関連した工作手段

「文化に関連した工作手段」は、国民のアイデンティティや価値観に直接作用するため、国内外の支持獲得、社会の分裂・混乱、世論の形成、アイデンティティの破壊など、長期的な影響力を持つ。また、目に見えにくく、抵抗されにくいという特徴がある。

---

30 内田泰「ウクライナ侵攻に学ぶサイバー攻撃、物理攻撃の前に重要システム不能化」『日経クロステック』2022 年 9 月 15 日、https://xtech.nikkei.com/atcl/nxt/column/18/02438/091500018/（2025 年 9 月 19 日閲覧）。

31 百度百家号《击“台独大本营” 多军种联合打击 3D 虚实动画发布》, https://baijiahao.baidu.com/s?id=1799902122318826057（2025 年 9 月 19 日閲覧）。

32 Global Times, PLA drills shock ‘Taiwan independence’ secessionist forces, May 26, 2024, https://www.globaltimes.cn/page/202405/1313033.shtml（2025 年 9 月 19 日閲覧）。

33 飯田将史「台湾を囲む中国による軍事演習―その特徴、狙いと今後の展望」『NIDS コメンタリー』第 325 号、防衛研究所、2024 年 5 月 28 日、4 頁。

特にハイブリッド戦においては、映画、音楽、文学などの文化的コンテンツをメディアやSNSを通じて展開することで、特定の価値観や歴史観を広め、相手国の国民の認識やアイデンティティに影響を与える効果を発揮する。

●「文化に関連した工作手段」の例

ロシアは、ウクライナ東部のドンバス地方に多くの在住するロシア系住民の人権が侵されていると主張し、軍事介入や政治支援を行い、国際社会に対して人道的介入としての正当性を訴えている[34]。

2022年以降の東部4州の「併合」においては、ロシア語話者の「意思」を根拠に住民投票を実施した[35]。また、ロシアによる占領地域ではウクライナ語教育を制限し、ロシア語教育を強化した。教科書の内容もロシアの歴史観に沿って改訂され[36]、若年層の文化的同化が進められている。

(6) 社会に関連した工作手段

「社会に関連した工作手段」は、民族対立、経済格差、政治的不満など、既存の社会的亀裂を煽ることで国家の統治能力を低下させる。特にハイブリッド戦では、フェイクニュースやSNSによる世論操作と組み合わせることで、社会の分断や不満を煽り、内部からの崩壊を誘導する。

民主主義国家では言論の自由の観点から言論統制が難しく、世論やマスメディアの影響力が大きいため、情報操作や心理戦に対して脆弱な側面が見られる。

●「社会に関連した工作手段」の例

ISILは、イラク戦争後の宗派対立やシリア内戦による治安の空白を突いて勢力を拡大し、2014年にはカリフ国家の建国を宣言した。彼らはテロ・ゲリラ・正規戦を組み合わせた戦術を展開するとともに、SNSを通じて若者を勧誘し、過激思想を拡散。さらに、宗派や部族間の対立を利用して社会的亀裂を煽り、国家の統治能力を低下させた。社会的弱者や不満層を取り込んで戦力化することで、外部からの軍事的圧力だけでなく、内部からの崩壊を促す構造を作り上げたのである[37]。

(7) 行政に関連した工作手段

「行政に関連した工作手段」は、行政機関に対する住民の不安や不満を煽ることで、行政への信頼を低下させることを目的とする。行政機関が保有するシステム、人材、対応能力に対する不安を助長する活動が行われる。

汚職は、発覚するまで相手にとって有利に働くため、隠密性の高い工作手段といえる。

---

[34] President of Russia, “Address by the President of the Russian Federation,” February 24, 2022, http://en.kremlin.ru/events/president/news/67843（2025年9月21日閲覧）.

[35] «Обращение Президента Российской Федерации» Президент России, 21 сентября 2022, http://kremlin ru/events/president/news/69390（2025年9月21日閲覧）.

[36] アムネスティ日本（2023年12月14日）「ウクライナ：子どもの将来への攻撃 ロシアの侵攻で制限される学校教育」https://www.amnesty.or.jp/news/2023/1214_10208.html（2025年9月21日閲覧）。

[37] 公安調査庁「『イラク・レバントのイスラム国』（ISIL）の退潮と今後の展望」、https://www.moj.go.jp/psia/ITH/topic/topic_01.html（2025年9月19日閲覧）。

特にハイブリッド戦では、行政機関のシステムに対するサイバー攻撃を通じて障害を発生させ、住民の生活に支障をきたすことで不満を煽る事例が散見される。

また、災害や事故などにおける行政対応は、住民の生命・財産に直結するため、SNS 等を活用して不安や不満を刺激し、行政機関を混乱させる工作も行われる。

●「行政に関連した工作手段」の例

2018 年 4 月、台湾の行政院情報セキュリティ処長である簡宏偉（チェン・ホンウェイ）氏は、台湾政府部門が毎月 2,000 万～4,000 万件のサイバー攻撃を受けていると発表した。2017 年には、政府系ウェブサイトの改ざんなど約 360 件の軽微な被害のほか、重要システムの停止や資料漏洩など 12 件の重大な被害が報告された。これらの攻撃の約 8 割が中国の「サイバー部隊」によるものとされており[38]、台湾住民の政府当局への信頼を損なわせることを目的とした工作と考えられる。

(8) 法律に関連した工作手段

「法律に関連した工作手段」は、武力行使を伴わず、国際法や相手国の法律を逆手に取ることで、合法的に見える形で影響力を行使する。民主主義国家では法的正当性が政策の根幹を支えるため、法的手段による攻撃は行動の制限、非難、弱体化に極めて効果的である。

特にハイブリッド戦では、法的主張をメディアや SNS で拡散し国際世論を操作する、経済制裁や関税措置を法的根拠に基づいて実施するなど、情報や経済と組み合わせて活用される。

●「法律に関連した工作手段」の例

中国は、国際法上の根拠がない「歴史的水域」として南シナ海のほぼ全域を自国の管轄水域と主張している。この主張は、2016 年 7 月に常設仲裁裁判所（PCA）が国連海洋法条約（UNCLOS）に基づいて下した裁定により否定されたが、中国はこの裁定に従わず、主張を撤回していない。

また、2021 年 2 月に施行された「中華人民共和国海警法」も例として挙げられる。この法律には、曖昧な適用海域や武器使用権限など、国際法との整合性に問題がある規定が含まれている。具体的には、「中国の主権・管轄権が外国の組織・個人から侵害された場合、武器使用を含む一切の措置を執る」と明記されている[39]。この記述自体は必ずしも国際法違反の内容とは言えないが、海警法施行以前から中国は南シナ海で周辺国の船舶に対して強硬な行動を繰り返しており、法の制定は新たな権限創設というより、強硬姿勢の喧伝による心理戦と位置づけられる。

このように、中国は国際法の解釈を恣意的に変更し、政治的目的を達成するために国内法を制定することで、一方的な現状変更を試みている。

---

38 「台政府部門每月遭遇二千萬次網羅攻擊 八成料來自大陸」自由亞洲電台、2018 年 4 月 5 日、https://www.rfa.org/cantonese/news/htm/tw-web-04052018074556.html（2025 年 9 月 19 日閲覧）。

39 中華人民共和国海警法第 22 条。

(9) インテリジェンス[40]に関連した工作手段

「インテリジェンスに関連した工作手段」は、国家の意図を達成するために秘密裏に行われる活動であるが、発覚しても国家が関与していないと主張できるような形で実施されることが一般的である。そのため、活動の兆候を察知することが非常に困難である。

この手段の判明事例は他の活動に比べ極端に少なく、表面化するケースは少ないと考えられる。特にハイブリッド戦では工作員を使って、現地メディアや SNS を通じて偽情報を拡散し、地元住民の不満を煽って政府への信頼を低下させる等、現地勢力と連携して暴動を支援するなどの活動が行われる。また、工作員が重要施設にアクセスし、マルウェアをサーバーに仕掛けるなど、サイバー攻撃との連携も見られる。

●「インテリジェンスに関連した工作手段」の例

台湾では 2024 年、中国の関与が疑われるスパイ事件により 64 人が起訴された。そのうち約 7 割にあたる 43 名が現役・退役の台湾軍人であり[41]、中国共産党の統一戦線部門などが台湾軍人を勧誘・脅迫し、軍事機密の収集や米国製輸送ヘリコプターの獲得を企てるケースもあったと報道されている[42]。

(10) 外交に関連した工作手段

「外交に関連した工作手段」は、軍事力を用いずに国際社会で影響力を発揮するための重要な手段である。外交・軍事力・経済力は、国家の国際的影響力を支える「三本柱」として相互に連携して機能するため、特にハイブリッド戦では経済・軍事に関連した工作手段との親和性が高い。

例えば、経済援助や軍事協力と組み合わせて相手国の政策に影響を与えるほか、外交官や政府関係者がメディアを通じてプロパガンダを発信することで、情報戦と連携し国際世論の形成に影響を与えることも可能である。

●「外交に関連した工作手段」の例

近年、経済的利益や中国との関係強化を目的として、台湾と断交し中国と国交を樹立する国が増加している。中国は友好国に対し、「一つの中国」原則の確認を求めたうえで、「台湾は中国の領土の不可分の一部である」と繰り返し主張している。近年の傾向として、中国は台湾統一への支持の同意を友好国に求めるようになってきている[43]。

2017 年 1 月には、ナウルが中国を国家承認したことで、台湾との国交を断絶し、台湾が

---

[40] 本報告においては、インテリジェンスという用語を、意思決定のための情報分析という狭義の意味ではなく、主に情報機関によって行われる諜報活動や隠密工作などを含めた広義の意味で使用する。

[41] 台湾国家安全局（NSB）「共諜案滲透手法分析」1-2 頁。
https://www.nsb.gov.tw/zh/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/ed8fddb8-3d99-4d3f-9414-c9b360f2df5a.pdf（2025 年 9 月 19 日閲覧）。

[42] 読売新聞「台湾が中国関与のスパイ最多の６４人起訴、軍関係者７割…中台統一目指し接触強化」2025 年 1 月 15 日 https://www.yomiuri.co.jp/world/20250115-OYT1T50020/（2025 年 9 月 19 日閲覧）。

[43] 福田円「「一つの中国」原則の行方」佐倉国際交流基金、2025 年 5 月 31 日、
http://www.sief.jp/21/2025/0531bundai.pdf（2025 年 9 月 19 日閲覧）。

外交関係を有する国は 12 か国に減少した[44]。

(11) 政治に関連した工作手段

「政治に関連した工作手段」は、政治に関与する人物を対象とするため、国家の方向性に大きな影響を与える可能性がある。一方で、活動の兆候を察知しにくく、公開情報では外国勢力による政治工作として認定された事例は非常に少ない。これは、活動の秘匿性が高いだけでなく、政府機関が一定程度把握していても公表できない事情があると考えられる。

特にハイブリッド戦では、支援する政治家に有利な情報を拡散し、対立候補に対してフェイクニュースを流すなど、情報操作と組み合わせた活動が行われる。

●「政治に関連した工作手段」の例

2024 年 12 月、同年 1 月に実施された台湾総統選および立法委員選挙に先立ち、中国当局が数百人の台湾の政治家に対して中国旅行を支援していたことが明らかになった。

台湾の法律では、選挙運動において中国を含む「外部の敵対勢力」から資金を受けることを禁じている。台湾当局者がロイターに語った情報によれば、各安保機関は過去 1 か月間に 400 件以上の中国訪問事案を調査し、その多くが村長など地元のオピニオンリーダーによるものであった。これらの訪問には、台湾政策を担う中国国務院傘下の組織から宿泊・交通・食事費用に対する補助金が支払われていたとされる[45]。

(12) インフォメーションに関連した工作手段

「インフォメーションに関連した工作手段」は、人々の思考、判断、価値観そのものに影響を与えるため、相手国の意思決定や社会の安定を揺るがす重要な手段の一つである。SNS や動画サイトを通じて偽情報や偏ったナラティブを拡散し、感情に訴える内容で世論を操作することが可能である。

近年では、生成 AI による偽動画・偽音声が本物と見分けがつかないレベルに達しており、印象操作の手段としても有効性が高まっている。民主主義国家では自由な言論空間が広く存在するため、こうした偽情報が拡散しやすく、真偽の確認に多大な時間を要する状況となっている。

特にハイブリッド戦においては、以下のような複合的な手法が用いられる。

・政府機関やメディアのウェブサイトに対する DDoS 攻撃や改ざんと同時に、SNS で偽情報を拡散し混乱を増幅する。
・軍事演習や部隊展開に伴い、「防衛措置」とするプロパガンダを発信する。
・経済制裁や輸出規制を実施しつつ、相手国の政策が原因であるとのナラティブを国際的に発信する。

---

44 外務省「台湾基礎データ」https://www.mofa.go.jp/mofaj/area/taiwan/data.html（2025 年 9 月 19 日閲覧）。

45 Yimou Lee「中国当局、台湾政治家数百人の旅行支援 総統選など控え＝関係筋」ニューズウィーク日本版（ロイター）、2023 年 12 月 1 日。
https://www.newsweekjapan.jp/headlines/world/2023/12/475397.php（2025 年 9 月 19 日閲覧）。

このように、インフォメーションに関連した工作手段は他の手段との親和性が高く、影響力を増幅させる効果を持つ。

●「インフォメーションに関連した工作手段」の例

2022 年 3 月、EU はロシアによるウクライナ侵略に関する偽情報を用いたプロパガンダを防ぐため、ロシア国営テレビ RT のヨーロッパ向け 5 チャンネルと、国営ラジオ・ニュースサイト「スプートニック」の EU 域内での提供を全面禁止する法律を制定した。これは、RT およびスプートニックが偽情報を拡散し、プーチン大統領が西側諸国を不安定化させるために利用していると判断されたことによるものである[46]。

(13) 技術に関連した工作手段

技術に関連した工作手段の中でも、GNSS（全球測位衛星システム）妨害は特に深刻な影響を及ぼす。GNSS 妨害は、強力な電波で正規の信号をかき消すことで受信機が測位不能となる。一方、GNSS なりすましは、本物より強い偽の信号を送信し、受信機を誤った位置や時刻に誘導するものである。

これらの攻撃により、以下のような社会インフラへの影響が生じる可能性がある。

・船舶の航路逸脱
・航空機の誤誘導
・金融システムの時刻同期エラー

特にハイブリッド戦では、GNSS なりすましとサイバー攻撃を組み合わせることで、ドローンやミサイルの誘導妨害、物流の混乱、金融システムの破壊などを引き起こす。また、GNSS 妨害による交通の混乱と偽情報の拡散を組み合わせることで、社会不安を煽り、政府への信頼を低下させることも可能である。

●「GNSS 妨害のよる工作手段」の例

2017 年 6 月、黒海付近において、20 隻以上の船舶が「なりすまし」GPS 信号によって誤った位置情報を表示する事案が発生した[47]。

また、ロシアは、現在も戦闘が続くドンバス地方に GPS なりすまし能力を有する R-330Zh ジーチェリ電子戦システムを度々展開させてウクライナ軍や OSCE（欧州安保協力機構）のドローンを妨害してきたことが報じられており、2019 年以降その妨害行為は増加している[48]。

これらの事例から、GNSS を対象とした妨害行為は高度化・大規模化する傾向にあることが示唆される。また今後の科学技術の発達により、量子工学やバイオテクノロジーなど、様々な先端技術が工作手段として使われる可能性にも警戒が必要である。

---

[46] Council of the European Union, “EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU,” Council of the European Union, March 2, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/（2025 年 9 月 21 日閲覧）.

[47] Dana Goward, “Mass GPS Spoofing Attack in Black Sea?” The Maritime Executive, July 11, 2017, https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea（2025 年 9 月 21 日閲覧）.

[48] “Russian GPS-Jamming Systems Return to Ukraine” Medium, May 5, 2019, https://dfrlab.org/2019/05/23/russian-gps-jamming-systems-return-to-ukraine/（2025 年 9 月 21 日閲覧）.

(14) その他の工作手段

本研究会では「選挙介入」については第 1～13 項で分析した工作手段が複合的に作用する事象であると捉えつつ、今後注目すべき手段として、あえて独立した項目として提示することとした。また、「生成 AI の影響」についても、既存の工作手段に横断的かつ深刻な影響を与える可能性が高いと判断し、追加項目として整理した。

【選挙介入】

選挙介入は、有権者の不安や怒りを煽る偽情報の拡散やプロパガンダによって世論を誘導し、投票行動に影響を与えるものである。具体的には以下のような手法が用いられる。

・候補者の信用を失墜させるためのスキャンダルやフェイクニュースの流布
・特定の候補者や政党への資金提供（政治的アクターへの支援）
・サイバー攻撃による投票集計の改ざん

これら複数の手段を組み合わせて実施される点において、選挙介入は典型的なハイブリッド戦の一形態といえる。

●選挙介入の例

米司法省モラー特別検察官の調査報告書によれば、2016 年米国大統領選挙に対してロシア政府による大規模かつ組織的な介入が認められたとされている。

ロシア軍参謀本部情報総局（GRU）は、民主党全国委員会（DNC）やヒラリー・クリントン陣営のメールをハッキングし、盗まれた情報を「DC Leaks」「Guccifer 2.0」「WikiLeaks」などを通じて公開した。

また、ロシアの「インターネット・リサーチ・エージェンシー（IRA）」は、SNS 上で偽情報や分断的なコンテンツを大量に拡散。Facebook 広告を活用し、特定の人種・地域・政治的傾向を持つ層に向けて情報を発信した。さらに、トランプ支持だけでなく、反トランプ運動（例：BLM）にも関与し、米国内の対立を煽ったとされている[49]。

【生成 AI による影響】

生成 AI は、従来の情報処理技術と比較して、スピード・規模・精度・個別化の面で著しい進化を遂げており、ハイブリッド戦における工作手段の高度化に大きな影響を与える可能性がある。以下にその具体的な影響を示す。

・生成 AI を用いて、サイバーウイルスなどを容易に作成できるようになり、サイバー攻撃の巧妙化・大量化が進む。
・テキスト、画像、音声、動画などを瞬時に生成できるため、偽情報やプロパガンダの拡散が加速し、SNS 等で情報の洪水が発生。真偽の判断が一層困難になる。
・ユーザーの属性や関心に応じて、個別に最適化されたメッセージを生成・配信し、対象者の心理に深く入り込み、行動変容を促す。
・LLM により、人間のような自然な言語で対話が可能となり、信頼性の高い情報源と誤認

[49] 川口貴久「ロシアによる政治介入型のサイバー活動～2016 年アメリカ大統領選挙介入の手法と意図」笹川平和財団「国際情報ネットワーク分析 IINA」https://www.spf.org/iina/articles/kawaguchi_01.html（2025 年 9 月 19 日閲覧）。

されやすく、説得力のあるストーリーや論理展開によって意図的な誘導が可能となる。
・自国に都合のいい情報や論説を大量にネット上に公開し、LLM の学習過程でバイアスを生じさせる試みが拡大しつつある。
・生成 AI が作成したコンテンツは、人間によるものと区別がつきにくく、言語の壁がなくなったことで発信源の特定が困難になりつつある。
・生成 AI は、人間の認知フレームを模倣することで、価値観や信念の形成に影響を与えることが可能である。

２　事例の分析結果

今回収集した事例をデータベース化し、工作手段ごとの傾向について分析を試みた。現時点では事例数が限られており、十分な網羅性には至っていないものの、初期的な傾向を把握する上で有益な示唆が得られた。

各工作手段における事例の特徴、頻度、影響の範囲などを整理した結果は、別紙 4 に示すとおりである。今後、事例の蓄積と分析の深化により、より精緻な傾向分析が可能となることが期待される。

第４章　中国による台湾強制統一ハイブリッド戦

１　懐柔路線と強硬路線

第１章第２項で示したパターン1からパターン3のコアとなるハイブリッド戦について、その位置づけは共通すると思われる。そこで、大きく「懐柔路線」と「強硬路線」に大別し、その具体的な目的等を推測し、研究の前提とする。

【懐柔路線】

台湾の親中化を進め、反中派を弾圧して本土との統一に向かう政権を樹立する路線を「懐柔路線」として設定した。そのため、台湾を支える機能、特に経済面で台湾の中国に対する依存度を高めさせ、中国なしには台湾が機能しない状況を作り上げるとともに、台湾を国際社会の中で中国の一部として受け入れさせるよう働きかけ、台湾全体を親中の方向に誘導する。

この路線が成功するためには、日米及びその友好諸国と中国の経済関係が切り離される傾向が続く中でも、中国経済が好調であることが前提となろう。その上で、日米等諸国と台湾の関係を悪化させるために、各国に対してもハイブリッド戦を実施する。

【強硬路線】

台湾内部の対立を煽ることにより内乱状態を生起させ、その混乱の中で本土との統一に向かう政権を樹立する路線を「強硬路線」として設定した。そのため、台湾を国際社会の中で孤立させるとともに、様々な手段で台湾の政治、経済、社会等の混乱を図り、極度に不安定な政治状況を作為し、必要があれば台湾の要請を受けて中国が治安部隊や軍を送り込むことも辞さず、事実上の統一を達成する。

この際、台湾が内乱状態となっても米国の介入が困難となるよう、日米を離反させるために、並行的に日米を対象としたハイブリッド戦を実施する。日米離反のためには、米中関係の現状に鑑み、対米強硬の一方で対日宥和策を採る可能性があるとした。

「懐柔路線」と「強硬路線」の関係の現実は、単純にどちらかの路線のみで推移していくとは思われず、この両者の間を揺れ動くものと考えられる。例えば、台湾における対中世論が厳しく「懐柔路線」がうまく機能しないような状況では「強硬路線」に移行するが、中国にとって状況が有利になればまた「懐柔路線」に戻るということも考えられよう。

以下では、ハイブリッド戦の各フェーズごとに「懐柔路線（左青線枠）」と「強硬路線（右赤線枠）」を比較検討する。（表 1）。

そのうえで、各路線の細部について具体的事例（Tool）をもって詳述する。

表１　強硬路線・懐柔路線の各フェーズにおける台湾に対するハイブリッド戦

懐柔路線	強硬路線
【条件形成フェーズ】 （Taiwan/Coaxing/Priming） TCP1：インテリジェンス活動 TCP2：親中政治家の取り込み TCP3：新中国派の取り組み TCP4：台湾の外交活動の妨害 TCP5：台湾との経済相互依存の強化 ・経済的アメとムチ ・インフラへの依存 TCP6：軍事的恫喝（弱） TCP7：日米への不信感助長 【不安定化フェーズ】 （Taiwan/Coaxing/Destabilization） TCD1：反中勢力の信用失墜 TCD2：対中連携の重要性宣伝 ・「平和フレームワーク」の宣伝 ・経済連携強化の協調 TCD3：米国への不信感の助長 【強制フェーズ】 （Taiwan/Coaxing/Coercion） TCC1：中国との結びつき強化 TCC2：台湾の情報空間の中国による支配 TCC3：選挙への公然・非公然の介入 TCC4：統一を主張する当局樹立	【条件形成フェーズ】 （Taiwan/Hardline/Priming） THP1：インテリジェンス活動 THP2：政治家への恫喝と信用低下 THP3：政治的・社会的分断 ・統一派・独立派の分断等 THP4：国際的組織からのボイコット THP5：台湾の経済的活動の妨害 THP6：軍事的恫喝（強） ・軍事演習、領空侵犯 【不安定化フェーズ】 （Taiwan/Hardline/Destabilization） THD1：台湾の行政能力不信助長 ・民間船舶航行妨害 THD2：社会不安、戦争への不安の助長 ・銀行、医療妨害、危機を煽る THD3：台・米・日の連携障害 ・海底電線の切断等 【強制フェーズ】 （Taiwan/Hardline/Coercion） THC1：社会、経済活動の混乱 ・重要インフラへ障害 ・軍事演習による経済活動妨害 ・経済活動妨害 THC2：台湾の情報発信の孤立化 ・通信ネットワークへ障害 THC3：内乱を作為 THC4：限定的軍事介入 ・軍隊の内戦への介入 ・島嶼部へのミサイル発射

出典：海洋安全保障研究委員会作成

２　台湾への懐柔路線

台湾への懐柔路線の各フェーズにおいて中国が台湾に対し実施するハイブリッド戦の概要は以下のとおりである。（細部は別紙 5 のとおり）

(1)　条件形成フェーズ

インテリジェンス活動、親中政治家の取り込み、新中国派の取り込み、台湾の外交活動の妨害、台湾との経済相互依存の強化、烈度の弱い軍事的恫喝、日米への不信感助長等を実施する。台湾の親中化のため、台湾内の指導層及び市民の取り込みを企図した

政治工作、メディア・コントロール、文化団体やシンクタンクへの財政支援等を行い、台湾内で親中的な世論を醸成する。さらに、台湾政権の親中度に応じ比較的烈度の弱い軍事的恫喝を行うとともに「日本は台湾の支援に懐疑的」、「米国は台湾を助けない」等の台湾の日米に対する信頼を低下させることを企図した中国に都合の良いナラティブ、偽情報の発信等を実施する。

(2) 不安定化フェーズ

反中勢力の信用失墜、対中連携の重要性宣伝、米国への不信感の助長等を実施する。ボット等を利用したサイバー空間での活動を含む偽情報、ナラティブ、プロパガンダの拡散、反中派の行動に見せかけた暴動や暗殺等の生起により台湾内で反中派を市民から孤立させる。また外交面でも一国二制度より多くの自治権を強調した「平和フレームワーク」の宣伝等により台湾を中国に引き寄せる一方、偽情報やプロパガンダの拡散により台湾の米国への不信感を助長し台湾を米国から離反させ外交的に孤立させる。

(3) 強制フェーズ

政治・経済・社会の各方面において情報空間での活動を含む多様な工作活動を実施する。台湾の親中派政権と中国との経済的枠組みの設立等により台湾を中国に経済的に依存させるとともに、台湾のインターネット空間や買収等を通じた台湾メディアの統制等により情報空間を支配することで親中派政権の樹立を後押しし、反中的な言説を封殺する。また、SNS 上でのボットの活用、反中勢力が政権をとると直ちに戦争状態になる等の偽情報を拡散等により台湾の選挙に介入する。さらに親中派への資金援助、反中派を弾圧するための警察能力強化のための支援、親中派政権による反中派取り締まりのための法制定の実施等を通じ、親中派政権の樹立・維持を支援し親中派政権による反中派の弾圧に協力し、反対意見を暴力的に封じる中で最終的に統一を決定させる。

3 台湾への強硬路線

台湾への強硬路線の各フェーズにおいて中国が台湾に対し実施するハイブリッド戦の概要は以下のとおりである。（細部は別紙 6 のとおり）

(1) 条件形成フェーズ

インテリジェンス活動、政治家への恫喝と信用低下、政治的・社会的分断、国際的組織からのボイコット、台湾の経済的活動の妨害、烈度の高い軍事的恫喝等を実施する。台湾内の対立を煽るため、政治家への信用失墜や選挙への不正介入等により政府と国民を分断する。またメディアの利用、大陸との宗教的つながりや外省人・内省人間の間隙等の台湾内に存在する社会的・文化的な亀裂の助長等により台湾を政治的・社会的に分断する。また親台湾的な国家との外交の妨害や国際組織・国際イベントから台湾を締め出すためのボイコット等により国際社会における台湾の外交的・経済的活動を阻害する。さらに台湾周辺での軍事演習、長距離ミサイルの発射テスト、中国軍その他の公的部門に属するアセットさらには海上民兵等による中間線を超えた活動等により戦争への不安を煽る。

(2) 不安定化フェーズ

台湾行政府の行政能力不信助長、社会不安及び戦争への不安の助長、台湾・米国・日本の連携障害等を実施する。金門・馬祖周辺での台湾船舶の航行妨害及び上空でのドローン飛行等の実施により台湾行政府に対しより緊張度の高い対応を迫ることでその行政能力に負担をかけ、台湾内での行政府への不信を増大させる。また、銀行、医療機関、交通・エネルギー・水道等の重要インフラに対するサイバー攻撃、海底電線の切断等の物理的破壊を含むインフラへの攻撃を実施し、社会不安を煽るとともに米国、日本等との連携を妨害する。さらに、台湾当局者が個人的な脱出計画を立てている等の危機感を煽る偽情報の流布、台湾周辺海域でのミサイル発射演習等より烈度の高い軍事活動の実施等により戦争への不安をさらに増大させる。

(3) 強制フェーズ

社会及び経済活動の混乱、台湾の情報発信の孤立化、内乱の作為、限定的軍事介入等を実施する。物理的破壊を含む台湾内の経済・社会・通信インフラへの攻撃を継続するとともに台湾接続水域内での中露共同演習の実施、大平島に対する接近封鎖等の軍事アセットをも活用したより強硬な台湾の経済活動に対する妨害を行う。また、海底ケーブルの切断や引き上げ局の破壊、データセンターや通信ネットワークへのサイバー攻撃、衛星回線への電子妨害等により台湾の情報発信を孤立化させる。そのうえで、台湾内で親中代理勢力による武装蜂起を伴う内乱状態を生起させ、親中勢力からの要請を口実とした台湾への部隊派遣を含む軍事介入を実施する。

第５章　台湾強制統一時の日本に対するハイブリッド戦

１　全般

台湾へのハイブリッド戦を基調に、日本に対するハイブリッド戦を「日台の離反（左青枠）」と「日米の離反（右赤枠）」に大別し全般を比較記述した（表 2）。

表 2　強硬路線・懐柔路線の各フェーズにおける日本に対するハイブリッド戦

日／台の離反を図る（懐柔路線を基調）	日／米の離反を図る（強硬路線を基調）
【条件形成フェーズ】 （Japan/Coaxing/Priming） JCP1：インテリジェンス活動 JCP2：台湾問題は内政問題と宣伝 JCP3：経済を含めた対日強硬工作 ・アジア経済における中国主導強化 JCP4：南西諸島近海、軍事演習での威嚇 JCP5：中台と沖縄一体とのナラティブ発信	【条件形成フェーズ】 （Japan/Hardline/Priming） JHP1：インテリジェンス活動 JHP2：日本の安全保障政策への干渉 JHP3：対米強硬の反面での対日宥和工作 JHP4：日本周辺海域での軍事演習 JHP5：沖縄を巡る世論の分断 ・米軍への不信感・不安感助長
【不安定化フェーズ】 （Japan/Coaxing/Destabilization） JCD2：日台連携強化を阻む工作 ・台湾経済からの日米の締め出し ・対中の経済連携強化をアピール JCD3：日台の意思疎通の妨害	【不安定化フェーズ】 （Japan/Hardline/Destabilization） JHD1：政府の行政能力不信助長 ・社会機能障害（限定的）による社会不安から政府不信助長 ・民間船舶保護に関し政府不信助長 JHD2：日米同盟のリスクを喚起 ・経済面での日中関係強化 ・日本が戦争に巻き込まれるリスク ・米中紛争のリスク JHD3：日米の意思疎通の妨害
【強制フェーズ】 （Japan/Coaxing/Coercion） JCC1：日本と台湾民主勢力の分断工作 ・「台湾は民主的に統一に向かう」偽情報 ・反中勢力に関するスキャンダル偽情報 ・統一の既成事実容認を条件に経済優遇 JCC2：統一に賛成の世論形成 ・国際的にも統一容認が大勢との偽情報	【強制フェーズ】 （Japan/Hardline/Coercion） JHC1：日米の分断工作 ・日米の機微な情報交換の妨害 ・自衛隊、在日米軍基地作戦能力の妨害 ・基地周辺住民の不安助長 JHC2：台湾への不介入の世論形成 ・「台湾で統一派が圧倒的優勢」偽情報 JHC3：「重要影響事態」等認定の遅延

出典：海洋安全保障研究委員会

2　対日本（日／台離反　台湾への懐柔路線を基調）

台湾への懐柔路線を基調とした、中国の日本へのハイブリッド戦の第一の目的は日／台離反であり、各フェーズにおいて中国が日本に対し実施するハイブリッド戦の概要は以下のとおりである。（細部は別紙 7 のとおり）

(1)　条件形成フェーズ

インテリジェンス活動、反中派の弱化と親中派の育成、経済を含めた対日強硬策、南西諸島近海での軍事演習での威嚇、中台と沖縄の一体性についてのナラティブの発信等を実施する。日台を離反させるため、サイバー・スパイを含む種々のインテリジェンス活動によって日台の分断、日本国内の重要インフラの脆弱ポイントに関わる情報収集を実施する。また政府その他の公的機関、経済団体等への要員の潜入、協力者の獲得等を行う。外交・経済面でも対日強硬策をとり、日本とアジア諸国の経済関係の妨害、福島第一原発の処理水の放出に対する強硬姿勢、台湾をも巻き込んだ尖閣諸島情勢の先鋭化等を実施する。さらに、南西諸島付近での中国軍による演習等の実施による軍事的威嚇、中国・台湾・沖縄の史的一体性についてのナラティブの発信等を行う。

(2)　不安定化フェーズ

日台連携強化を阻む工作、日台の意思疎通の妨害等を実施する。台湾及び日米企業に対する圧力の強化、台湾の多国籍企業に対する広範な制限等により台湾経済から日米を締め出す。また、漁船等を利用した海底ケーブル切断、尖閣諸島情勢の先鋭化特に日本の海上警備行動の発令を契機とした台湾内の反日世論の惹起、台湾は日本に期待していないとの偽情報の拡散等により日台の意思疎通を妨害する。

(3)　強制フェーズ

日本と台湾民主化勢力の分断工作、日本国内における統一に賛成の世論形成等を実施する。SNS 上でのボット活用等のサイバー・オペレーションを含む多様な方法により「台湾は民主的に統一に向かう」、「国際的にも統一容認が大勢」等の偽情報を拡散する。また、日本に対し統一の既成事実を認めない場合は経済制裁を実施する等の経済に関連した強圧的な手段をとる。

3　対日本（日／米離反　台湾への強硬路線を基調）

台湾への強硬路線を基調とした、中国の日本へのハイブリッド戦の第一の目的は日／米離反であり各フェーズにおいて中国が日本に対し実施するハイブリッド戦の概要は以下のとおりである。（細部は別紙 8 のとおり）

(1)　条件形成フェーズ

インテリジェンス活動、日本の安全保障政策への干渉、対米強硬の反面での対日宥和工作、日本周辺海域での軍事演習、沖縄を巡る世論の分断等を実施する。サイバー・スパイを含む種々のインテリジェンス活動によって自衛隊、在日米軍の脆弱ポイント、日本国内の重要インフラに関わる情報収集を行い、また政府その他の公的機関、経済団体等への要因の潜入と協力者の獲得等を実施する。外交・経済面では経済的見返りの供与、尖閣諸島情勢での態度軟化等により日本に対し秋波を送る。また、日本周辺海域に

おいて日本に対し直接的な脅威となる演習の実施回数を減らしつつ米軍部隊に対しては挑発的な演習を実施することにより、日本国民の間に不安感を醸成する。さらに、日米同盟は日本の安全に寄与せず戦争への巻き込まれリスクを増加させる、米国は中台紛争に介入しないといった米国の行動に関連するナラティブ・偽情報の流布、沖縄での米軍人による犯罪に関するバイアスをかけた情報や偽情報の発信等による米軍への不信感・不安感の助長、中国と沖縄の歴史的つながりや沖縄戦に関するナラティブの拡散による日米両政府に対する信頼感の棄損等を実施する。

(2) 不安定化フェーズ

日本政府の行政能力に対する不信の助長、日米同盟のリスクの喚起、日米の意思疎通の妨害等を実施する。サイバー・オペレーション等による銀行や病院におけるシステム障害の発生、大量の中国漁船の日本 EEZ への侵入、法執行と軍事活動の曖昧性の利用等の手段を用いて、日本政府の行政能力に対する不信を助長する。また経済面で日本を優遇する一方、軍事面においては米軍基地に対するミサイル・航空攻撃を模擬した演習の実施、第二列島戦越えのミサイル発射演習の実施等により米中紛争のリスクや日本が戦争に巻き込まれるリスクを強調し、日本国民の間に日米同盟をリスクとしてとらえる世論を形成する。さらに、漁船等を使用した海底ケーブルの切断により日米間の情報共有を妨害する。

(3) 強制フェーズ

日米の分断工作、台湾有事への不介入の世論形成、「重要影響事態」等認定の妨害等を実施する。電子戦、サイバー攻撃等の手段により海底電線による通信、衛星通信等を阻害し日米の情報交換に障害を発生させ、また日本国内の電力、ガス、水道等の重要インフラを攻撃しそれに依存する自衛隊、在日米軍の作戦能力を低下させる。さらに「台湾で統一派が圧倒的優勢」等の偽情報を拡散することで日本国内で台湾有事への不介入を支持する世論を形成し、また「「重要影響事態」等の認定は中国に対する戦争行為である」とのプロパガンダにより日本政府による「重要影響事態」等の認定を妨害する。

4　中国が日本に対して行使する各ハイブリッド手段

中国が日本に対して行使する各ハイブリッド手段及び標的とされる日本のドメインを分析した結果は別紙 9 のとおり。

第６章　米国と他国へのハイブリッド戦

１　米国へのハイブリッド戦

【台湾への懐柔路線基調の場合】

台湾への懐柔路線を基調とした場合の中国の米国に対するハイブリッド戦の第一の目的は、米国が親中化する台湾に不信感を持ち、台湾を支援する意思を減じさせることにあると考えられる。そのため、以下を目標に各種のハイブリッド手段を行使するであろう。

・反中派を弾圧する台湾当局及び親中化する住民に対する米国内の不信感を助長
・武力を用いない統一について、米国が事態に関与する必要があるのかという議論を米国内で扇動
・経済面で中台一体化を前提とした対応を強要（経済的なアメとムチを駆使）
・米台間のコミュニケーションの阻害（物理的通信阻害、情報操作等）

【台湾への強硬路線基調の場合】

台湾への強硬路線を基調とした場合の中国の米国に対するハイブリッド戦の第一の目的は、台湾での内乱状態に米国が介入できないようにすることにあると考えられる。そのため、以下を目標に各種のハイブリッド手段を行使するであろう。

・米国内での台湾に対する不信感増大、支持低下
・戦争のリスクに関する米国内の不安感増大（軍事リスクの他、経済面も含む）
・台湾に関して内政不干渉の原則が適用されるとの国際世論、米国内世論の喚起
・日本に対する不信感・不満の増大、特に在日米軍基地使用に関する不透明感増大
・日米間のコミュニケーションの阻害（物理的通信阻害、情報操作等）
・米比連携の切り崩し、特に比基地使用に関する不透明感増大

２　米国以外の関連諸国へのハイブリッド戦

台湾への懐柔路線を基調とした場合、中国は中台統一を国際的に正当化し、これを支持する国々を多数派にするための工作を行うであろう。

そのため、いずれの路線の場合でも、情報操作、ナラティブ拡散、経済的誘導（アメとムチ)、国際機関の利用（中台一体加盟等）等、各種のハイブリッド手段を行使すると考えられる。

また強硬路線を基調とした場合、中国は台湾で内乱が生起したとしてもそれは中国の内政問題であり、米国をはじめとする他国が介入すべきではないという国際世論を形成しようとするであろう。

具体的には、上記各種ハイブリッド戦を関連諸国に行使することにより、以下を目標に多国間連携を切り崩すであろう。

・ASEAN+3、ASEAN 地域フォーラム（ARF）等のマルチラテラルな協力及び QUAD、AUKUS、

日米豪や日米韓等のミニラテラルな協力の切り崩し
・ASEAN 諸国、特に南シナ海周辺国の切り崩し
・太平洋島嶼国への関与拡大による切り崩し

第７章　ハイブリッド戦に対する台湾の各ドメインの脆弱性

【外交】

・中国の「一つの中国原則」により、国際機関への参加が制約されるとともに、正式な国交を持つ国が少なく、外交活動が限定されている

・そのため、各国と連携して行う国際活動や被支援についても制約を受ける

【政治】

・恒常的に親中・反中勢力の対立があり、常に政治的分断が激化するリスクが存在する

・選挙において、中国の利益誘導や偽情報拡散などの介入を受ける可能性がある

【文化】

・中国文化との歴史的・言語的近接性を利用して、中国が文化的影響工作（映画、音楽、出版など）を仕掛けやすい素地がある

・媽祖信仰など大陸側と共通した民間信仰を通じて影響工作を受けやすい

【社会】

・1949 年中華民国政府が台湾に移転した際に流入した外省人が、既に台湾に居住していた内省人を弾圧した歴史があり、その確執が未だに社会に内在している

・地震、台風等による災害が多いため、これに乗じた偽情報等で社会が混乱する可能性がある

【法律】

・中国の「一つの中国原則」によって、国際法上の地位が曖昧にさせられている

・中間線や防空識別圏などを巡り、中国が既成事実化による無効化の試みを継続

【軍事/防衛】

・中国との軍事力格差が大きい中、米国の曖昧戦略により抑止効果に不安が存在

・軍事的防衛の基本的な考え方について、政府・軍内においても早期撃破と持久のどちらを重視するかなど様々な方針が存在し、防衛力整備などを巡って対立が生じる素地が存在

・宇宙・無人機・サイバー・電磁波なども含めた多領域横断能力の整備に遅れ

・台湾軍は内部の制度改革や政治的中立性の課題に直面しており、中国からの影響工作を受けやすい。

【宇宙】

・宇宙開発の予算・技術力が限定的で、独自衛星網の整備が遅れているため、他国への依存度が大

【行政】

・与野党の強い確執が、中央と地方の両方において存在するため、一貫した行政施策の実現が困難になるなど、脆弱性を抱えている

・デジタル行政が進んでいるが、セキュリティ体制が追いついていない

【インフラ】

・電力・物流・医療などが高度にデジタル依存し、サイバー攻撃に脆弱

・海外とのインターネット通信において海底ケーブルへの依存度が高く脆弱
・エネルギーの 9 割以上を輸入に依存し、供給途絶のリスクが高い

【経済】

・半導体産業への依存度が高く、原料輸入・製品輸出が途絶すると経済リスク大
・中国との経済関係が密であり、経済面での制裁及び懐柔の両面に弱い

【インテリジェンス】

・歴史的に、外省人対内省人、国民党対民進党の対立がある中で、中国のスパイ活動に脆弱な土壌が存在
・中国側の諜報・防諜体制と比較して、民主主義であるが故の弱点が存在

【インフォメーション】

・政治論争において SNS が果たす役割が大きい社会であるという特性上、ネット空間における偽情報拡散等の情報操作に影響されやすい
・親中国メディア（中国によって買収されたメディアを含む）による一定の影響力がある

【サイバー】

・中国の圧倒的なサイバー攻撃能力に対しサイバー防衛が後手に回る傾向にある
・行政のデジタル化が進んでいるために、サイバー攻撃を許した場合に影響が大
・サイバー防衛における国際協力の枠組みが制度化されていない

第８章　ハイブリッド戦に対する日本の各ドメインの脆弱性

中国が台湾の強制統一を狙って、台湾に対すると同時に日本に対してもハイブリッド戦を仕掛けてくることを想定した場合の、日本の各ドメインの脆弱性について、以下の通り分析した。

【外交】

・日米同盟を基軸としつつも、世論には対米不信感が根強く存在。経済的、外交的揺さぶり、危機への社会不安等によって、対米不信へと世論が大きく傾く可能性
・尖閣諸島をめぐる情勢は、中国政府及び台湾当局が尖閣諸島に関する独自の主張を行っていることから複雑化する可能性

【政治】

・中国との経済的利益を背景とした対中国配慮、米国の厳しい対中国経済政策との政治的ジレンマに陥る可能性
・一部の政治勢力の根強い反米意識を利用し、スキャンダル、経済支援等による親中に取り込まれる可能性

【文化】

・沖縄と本土の認識のギャップを利用される可能性
・中台と沖縄がもともと同一の文化圏であるとのナラティブ発信が強化されると、台湾も沖縄を日本から切り離そうとしているとの台湾不信助長につながる可能性

【社会】

・周辺海域へのミサイル等の発射による軍事的恫喝、偽情報の拡散、サイバー攻撃等により、特に基地周辺住民の不安感を募り、反基地闘争に広がる可能性
・台湾情勢の不安定化によって大量避難民が日本に押し寄せてくる可能性と、偽情報の流布により社会不安に陥る可能性
・南西諸島が戦火に巻き込まれる可能性と、偽情報の流布により社会不安に陥る可能性

【法律】

・存立危機事態を認定した上での各種の対処措置（究極的には防衛出動を含む）に関して、国会承認を巡って政治的に紛糾する可能性
・米国が武力介入を行う準備を開始した際、重要影響事態を認定した上での自衛隊の各種活動に関して、国会承認を巡って政治的に紛糾する可能性
・尖閣諸島情勢を巡る日本の海警行動が、日本側による一方的な軍事作戦であるとの中国側のプロパガンダに利用され国際的な誤認識が生ずる可能性、またこれによって台湾においても日本に対する批判が強まり、中台の連携強化のためのプロパガンダとして、台湾における世論操作に利用される可能性

【軍事/防衛】

・米国への対中戦略への寄与（重要影響事態）と日本防衛（防衛上の事態）が併存する可能性
・台湾危機における南西諸島住民避難と難民保護の混乱の可能性

・日本の領海・領空侵犯、日本周辺での軍事演習の活発化は社会の不安と同時に強硬派を煽り社会が分断される可能性があるのみでなく、関係機関の警戒監視等の負荷を増し、防衛資源を疲弊させる可能性
・GPS 信号の欺瞞と偽情報は警戒監視等にも直接的な影響を与え、誤判断それに伴う対応を誤る可能性
・核の恫喝により米国の核抑止への信頼性が揺らぐ可能性がある

【宇宙】
・宇宙を利用した日米の指揮通信機能の障害により、日米間の意思疎通障害につながる可能性
・通信、測地（GPS）、情報等、社会生活の多くの部分が宇宙インフラに依存しており、衛星への妨害活動が社会不安、政権不信につながる可能性

【行政】
・中国海警局船舶による日本の民間船への妨害等、海洋国家として各種海洋権益の保護への対応で政府への不信が助長される可能性
・南西諸島住民の住民保護等の安全確保に関する不安から、政府への不信が助長される可能性

【インフラ】
・在日米軍、自衛隊の基地機能は民間インフラ（電力、水道、ガス、物流）に依存しており、特に実施主体が不明なサイバー攻撃により障害は、日米連携の信頼性に不安をもたらす可能性
・日本、台湾ともに海底ケーブルへの依存度が高く、海底ケーブルの障害は、日米、日台間の政策連携に障害をきたす可能性

【経済】
・日本経済の対中国依存度が大きいことから、硬軟合わせた経済的ゆさぶりが政治的ゆさぶりにつながる可能性
・台湾との半導体技術の連携に関して、ゆさぶりをかけられる可能性

【インテリジェンス】
・台湾に関するインテリジェンスのソースが限定されていること、また通信障害により台湾との情報が遮断（孤立）されたときには、日米台の認識の齟齬を誘発する可能性

【インフォメーション】
・国内のインフラ障害に関する偽アカウントを利用した偽情報の大量拡散と同時並行的なサイバー攻撃、あるいは台湾、米国、国際社会に関する、特に AI を利用したフェイク画像等の偽情報の大量拡散は社会不安を募り、国内世論を分断させる可能性
・サイバーあるいは工作員による隠密活動は、気が付いた時には手遅れになる可能性

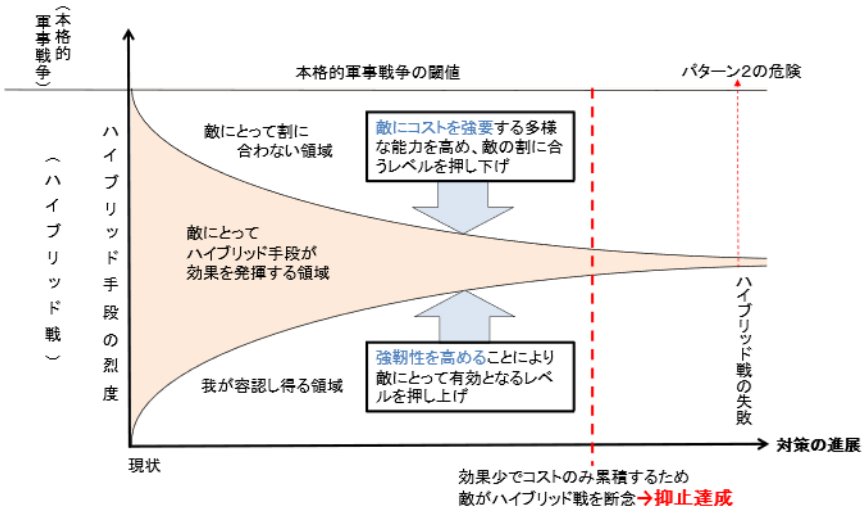
【サイバー】
・ウクライナ侵略において、深刻なサイバー事態の対応に米国等の官民支援が重要であったと言われている。日本の場合、支援を受け入れる際の法制、制度及び役割分担等に関して平素から協議しておかないと、危機時に混乱する可能性

・国家主体が関与する可能性のある、サイバー安全保障事案に対応が遅れる可能性
特に、中国には国家を背景としたサイバー集団が散見されており、国家の関与を曖昧にしたサイバー攻撃への対応が遅れる可能性
・サイバー戦と電磁戦は不可分であるにもかかわらず、日本の電磁波管理制度において安全保障上の考慮が不十分な点に付け込まれる可能性

第９章　ハイブリッド戦対策の基本的考え方と多国間連携の重要性

第 1 章でも指摘したように，ハイブリッド戦への対処として、あらゆる手段の行使を未然に防ぐということは現実的ではない。各分野においてそれ以上に事態が進展しないよう種々の対策を講じて、攻撃側が最終的に目的を達成する以前の、努めて初期の段階で諦めさせ、状況を安定化させることが重要である。

図 5　ハイブリッド戦抑止の概念図



出典：Vytautas Kersanskas, "op cit", p.12, figure1.に基づいて作成

ハイブリッド戦に関するリトアニアの研究者ケルサンスカスは、この観点から非常に有意義な考え方を提示している[50]。それによると、ハイブリッド戦の各種手段が有効に働く条件は、その脅威手段が相手の社会に実際にマイナスの影響を与える程に烈度が高くなくてはならないと同時に、相手側から武力行使を含む決定的な反撃を受ける烈度よりは低くなくてはならない。すなわち効果が上がる最低烈度と、反撃を受ける最高烈度の間の領域でハイブリッド手段を行使することが、攻撃側の勝ち目だというのである。これを逆に防衛側の立場から見ると、各種のハイブリッド手段に対する社会としての強靭性を高めて攻撃を無効にすると同時に、反撃発動のレッドラインを下げるようにしていけば、図 5 のようにその間に挟まれたハイブリッド手段の有効領域はどんどん狭まっていくことになる。

この防衛側からの反撃を、大規模な軍事力による攻撃として想定し、力によるレッドラインとして強く示して抑止すべきだという議論も理論的にはあり得よう。しかしそれでは、第 1 章で指摘したパターン 2 による本格的軍事戦争を抑止するどころか、こちらから望ま

[50] Vytautas Kersanskas, “DETERRENCE : Proposing a more strategic approach to countering hybrid threats”, Hybrid CoE Paper 2, March 2020. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf.

しくない軍事戦争を起こすことが前提となってしまう。したがってこのレッドライン引き下げとは、大規模な軍事力で反撃する閾値を引き下げるのではなく、小規模な軍事力による対応を含めつつも、主として非軍事の各分野で中国側に耐えきれないコストを課す外交的、経済的制裁など、多様な手段の組み合わせによる反撃の発動ラインとするのが現実的であろう。図 5 で「敵にコストを強要する多様な能力を高め、敵の割に合うレベルを押し下げ」と記述しているのがこれに当たる。

ハイブリッド戦の各種手段は、相手国の政治、外交、経済、社会、文化、情報、軍事など各ドメインに存在している脆弱性を狙ってくる。例えば、国内に存在する政治的対立を助長する手段、外交面で頼りにしている国との関係を悪化させる手段、経済的に弱みとなっている海外のサプライ・チェーンを破壊する手段、地域間に存在する歴史的対立を助長する手段、SNS 等に依存した流動的な情報環境を操作する手段、軍事面での弱点を国民に暴露する手段などを複合的に用いて、弱い所から亀裂を広げていくことにある。

したがって、日米台などが、それぞれ各分野での脆弱性を低減し、強靭性を高める施策を採ることは、各種のハイブリッド手段の有効性を減じ、より烈度の高い手段を用いなくては効果がないという状況を生むことに繋がる。これに対抗して、中国側がより烈度の高い手段を行使すれば、国家の関与を秘匿することはより困難になる。そこで日米台の側としては、個々の手段に対して中国が高いコストを払わざるを得ないような制裁等を課していくことが、ハイブリッド戦のそれ以上のエスカレーションを抑止することにつながる。この際、中国側のハイブリッド手段の一つ一つを検知する都度直ちにコストを付加し、各種コストの累積効果で全体として中国が耐えられないような状況を作ることができれば、抑止はより効果的なものとなる。

これを全体として見れば、ハイブリッド戦が始まることを抑止することは不可能だが、一つ一つのハイブリッド手段の行使に対し、我の側の強靭性を高めることでその効果を減じるとともに、その都度相手にコストを付加してその継続をためらわせることで、相手側のハイブリッド戦による試みを中途で断念させることは可能と考える。

中国による台湾強制統一をハイブリッド戦の段階で拒み、ついにはこれを断念させて状況を安定させるためには、日米台側の政治、外交、経済、社会、文化、情報、軍事など各ドメインにおいて脆弱性を減じ、強靭性を高める施策を早急に進めるとともに、中国によるハイブリッド手段の行使を早期に検知しその狙いを総合的に判断できる態勢を整え、その判断の下に個々のハイブリッド手段の行使に対して着実にコストを付加できる国際的な枠組みを整えることが急務である。

そのためには、これらを日米台がそれぞれ行うだけではなく、オーストラリア、フィリピン、韓国、ASEAN・欧州・大洋州の同志国などと連携して行うここことが必要である。

第 10 章　中国による台湾統一阻止のための多国間連携に関する提言[51]

1　日台等の脆弱性を減ずるための多国間連携

(1)　安全保障・軍事的枠組み

ア　同盟・同志国連携の強化

・ハイブリッド戦への対処に重点を置いた軍事情報共有や二国間・多国間演習により、参加国間の相互信頼関係及び対応能力を強化する。この際、日米豪印（QUAD）にフィリピン・ベトナム等を連携させるなど、多様な枠組みの活用に留意する。

イ　同盟・同志国との整合のとれた「戦略的コミュニケーション」

・同盟・同志国による実践的なシナリオ演習などを通じた行動を通じた抑止・対応措置と、誤解を招かぬよう冷静かつ正確な情報のタイムリーな発信を組み合わせることで、安定に資する質の高い「戦略的コミュニケーション」を実現する協力体制を構築する

・台湾周辺海域での航行の自由を守るための取組の継続的実施

ウ　抑止力の可視化

・比の法執行能力、海洋監視能力の一層強化のために日本による防衛装備品の移転を積極的に推進する。この際、このような能力強化が緊張を高めるものではなく、地域の安定に寄与するものだとの認識共有に努める。

・台湾軍と各国軍の間での公式、非公式の交流機会を増大させ、先端技術、新領域、政軍関係などに関する知見を共有する

・台湾の災害を想定した多国間共同訓練の作為

(2)　経済・インフラの強靭化

ア　経済封鎖への備え

・中国があくまで台湾地域に主権を持つ国としての法執行だと主張して台湾を事実上海上封鎖したとしても、これが国際的な政治・経済秩序に反するものだとの認識を共有し、西太平洋における海上輸送の安全確保に向けた国際協力を推進する

・台湾の半導体・衛星技術に対する国際的バックアップ体制の構築

・エネルギー供給源の多様化に向けて、各国との協力を強化する

イ　サプライ・チェーンの再編

・中国依存の高いサプライ・チェーンからの脱却を目指し、パックス・シリカ[52]のような協力枠組みの構築などを通じて、国際的市場の多様化を促進する

ウ　経済支援・連携

---

[51] 日本の脆弱性を減ずるために日本が独自に行うべき対策については、海洋安全保障委員会 2024 年度研究報告の「第 6 章 ハイブリッド戦における日本の脆弱性を踏まえた政策提言」において詳述したので、同研究報告を参照されたい。
https://www.npi.or.jp/research/data/npi_policy_maritime_security_20250331.pdf 。

[52] パックス・シリカとは、AI に不可欠な半導体や重要鉱物などのサプライ・チェーンの安定化・強化を目的として、2025 年 12 月に立ち上げられた米国、日本、韓国、オーストラリアなどによる多国間協力枠組み。

・台湾がグローバル・サウス諸国との経済連携に積極的に参加できるよう支援や共同での経済活動を強化する
・太平洋島嶼国が持つ戦略的価値を踏まえ、日本独自及び同志国と連携した経済支援を積極的に展開する
エ　インフラの強靱化
・太平洋地域における海底ケーブルの安全性を確保するため、国際的な連携体制を構築する
・宇宙配備及び地上配備の宇宙関連アセットの安定的利用についての国際連携を強化する
・各国のデータセンターの強靭性を高めるため、国境を越えたバックアップ体制の構築などに関し協議を開始する。

(3) 外交・制度的枠組み

ア　既存の国際枠組みの活用
・既存のグローバル協力訓練枠組み（GCTF）[53]などの枠組みを活用し、台湾の国際的地位をより安定的なものとし、日本として準公的な関係を拡大する素地を作る
・台湾の国際機関参加（WHO、ICAO など）への支持表明とロビー活動
・台湾の国際機関参加支援と外交関係を持つ国への支援を協力して実施
イ　国際法と規範の強化
・東シナ海や南シナ海において、領有権や管轄権に基づく境界が確定していない海空域での衝突を防止するための軍及び法執行機関の行動規範を定める国際協議を促進
・台湾海峡の安全航行に関する国連海洋法条約（UNCLOS）の遵守強化

(4)　宇宙・サイバー・電磁波領域の連携

ア　技術協力の推進
・宇宙・無人機・電磁波など新領域の脅威に対応するため、同盟・同志国との技術協力の推進
・台湾への衛星技術提供に向けた枠組みを構築し、日本がその支援を主導する
イ　サイバー脅威等への対応
・サイバーの問題は一国で到底解決出来ない、平素から各国との情報共有の枠組みを構築するとともに、顔が見える関係を構築するためにも人材の交流を促進する必要があり。
・サイバー空間や情報空間などにおける新しい脅威に対処するための国際法の適用に向けた国際協議を促進

(5)　情報空間における連携

ア　価値観を同じくする同盟・同志国が連携して共通のナラティブを発信

---

[53] グローバル協力訓練枠組み（GCTF）とは、2015 年に米台間で立ち上げられた人材育成の枠組みであり、現在では日豪加も参加している。この枠組みを通じて、公衆衛生や環境問題など地域の共通課題について、東南アジアや大洋州諸国を中心に各国から担当官や専門家を招いたワークショップ開催など、交流を深める活動が行われている。

・中国が自国の一方的な主張に関する各種のナラティブを世界に発信していることを踏まえ、自由や民主主義という価値観を共有している同志国が連携して共通のナラティブを世界に発信

イ　中国による偽情報や恣意的情報の拡散を無効化するための協力強化

・中国が偽情報（disinformation）や、事実に基づいていても恣意的な一方的解釈に偏った情報（malinformation）を広めようとすることに対し、同志国が正しい情報の即時的発信やファクトチェックなどでこれを無効化するために協力

(6)　ハイブリッド脅威への総合的な対応

ア　多国間ハイブリッドシナリオ演習の推進

・各国とのセミナー等を通じて、ハイブリッド戦とは何かの認識の共有を図る必要がある。その上で多国間でのハイブリッド戦を想定したシナリオ演習を実施し更なる認識の共有を深める。

イ　多国間情報共有ネットワーク

・中国による偽情報・サイバー攻撃などに包括的に対応するための多国間情報共有ネットワークを構築する。

ウ　ハイブリッド脅威対策センターの構築

・将来的には東アジア地域に「ハイブリッド脅威対策センター」を設置、ハイブリッド脅威に関する、情報共有・対策の恒常的協議体を構築

２　中国によるハイブリッド攻撃にコストを課すための多国間連携

・小規模なものであれ、中国による武力行使や過激な軍事行動、警戒監視のための艦艇・航空機に対する挑発的行為などに対して、国際的な批判を強めるとともに、海上衝突回避規範[54]のように自制を求める国際的枠組みを更に推進して圧力を強化

・中国による経済的な圧迫に対し、各国が連携して、貿易、投資などの分野で対抗的な措置を実施

・海底ケーブルや航空宇宙インフラ等の破壊に関し、中国の関与が判明した場合には、関係国際機関においてペナルティを課すことを検討

・中国による国際法違反の行為に対し、国際司法裁判所等に提訴する等の圧力をかけることによって、国際的な包囲網を形成

・サイバー攻撃に関する中国政府の関与が判明した場合には、能動的サイバー防御やそれに類似する活動において、連携して措置を発動し攻撃元を無害化

・各国間での情報共有に基づく総合的分析の結果、中国が複合的な手段によるハイブリッド攻撃を仕掛けていることが疑われる場合、その事実を示して中国の国際的孤立を図る

---

[54] 海上衝突回避規範（CUSE）とは、2014 年の西太平洋海軍シンポジウム（WPNS）において、中国を含む 21 ヵ国によって合意された海上での偶発的な軍事衝突を避けるための規範であるが、対象が海軍艦艇・航空機に限定されている他、法的拘束力もない。

とともに、共同での対抗措置を検討

研究を終わるにあたって、今後取り組むべき方策

3 年間にわたり、中国が実施する可能性のある台湾へのハイブリッド戦を例として研究した。まだまだ研究の途上でもあり多くの課題があるが、微力ながら当研究会として取り組んだ方策、今後取り組むべき方策について列挙してみる。

1　日本国内での対応に向けた取り組み

【国民への啓発（動画配信）】

研究当初ハイブリッド戦とは何かとの議論から始まった、またこの様な研究を公開することが果たして国益につながるのかとの議論もあった。しかし各国の研究者との意見交換を通じ、まずは新たな脅威についての国民の理解が重要であるとの認識のもと、「ハイブリッド戦とはなにか」という動画配信を試みることにした。

【国民への啓発（事例のデータベースサイト作成、維持管理）】

事例のデータベースサイトを Web（日本、英語）上に公開することを試みた。本データベースサイトはまだまだ発展途上であり、充実させるために今後どの様に本データベースサイトを維持管理していくかの課題がある。

【事例等の更なる分析（AI の活用）】

今回は 40 の Tool を基本にして研究したが、果たしてこれで十分なのか、さらに深掘りしていく必要である。同時に生成 AI 等を活用した事例の更なる分析手法についても研究する必要性があり、今後の課題である。

【省庁横断による脆弱性の解決】

日本のハイブリッド脅威への脆弱性を分析した、脆弱性は各省庁多岐にわたっており、省庁横断的に対応する体制の構築が求められる。

2　多国間としての対応に向けた取り組み

【同盟・同志国との認識の共有（セミナー・簡易な演習）】

各国とのセミナー等を通じて、例えば 40 の Tool の各国の抱える具体的事例（課題）を共有し、ハイブリッド戦とは何かの認識の共有を図る必要がある。

そのうえで、同盟・同志国によるハイブリッド戦を想定した簡易なシナリオ演習を実施し更なる認識の共有を深める必要がある。

【同盟・同志国との戦略的コミュニケーションの強化】

同盟・同志国による実践的なシナリオ演習を通じ、偽情報やプロパガンダへの対抗策として、信頼性の高い情報発信等「戦略的コミュニケーション」に関する協力体制を構築する必要がある。

【同盟・同志国との技術的協力の強化】

インフラの防護やマルウェア対策などの連携等、特にサイバー防衛技術の共同開発の構築等に、多国間の協力体制を構築していく必要がある。

【東アジア地域にハイブリッド脅威対策センターの構築】

将来的には東アジア地域に「ハイブリッド脅威対策センター」を設置、ハイブリッド脅威に関する、情報共有・対策の恒常的協議体を構築する必要がある。

ハイブリッド脅威は、国家の境界を越えて社会の隅々に影響を及ぼす。ゆえに、対応もまた境界を越えた連携が求められる。本研究はその第一歩であり、今後の政策形成・技術開発・国際協力の礎となることを願ってやまない。

最後に本研究の機会を与えていただいた、外務省に謝意を表したい。

別紙 1

ハイブリッド脅威活動のツールと影響を受けるドメイン

	ツール	影響を受ける可能性のあるドメイン
1	インフラに対する物理的打撃	**インフラ**、経済、サイバー、宇宙、軍事／防衛、情報、社会、行政
2	インフラへの依存（民軍間の依存を含む）の構築と利用	**インフラ**、経済、サイバー、宇宙、軍事／防衛、行政
3	経済的依存関係の構築又は利用	**経済**、外交、政治、行政
4	外国への直接投資	**経済**、インフラ、サイバー、宇宙、軍事／防衛、行政、インテリジェンス、情報、政治、法律
5	産業スパイ	**経済**、インフラ、サイバー、宇宙、インテリジェンス、情報
6	相手国経済活動の阻害	**経済**、行政、政治、外交
7	経済的困窮の利用	**経済**、行政、政治、外交
8	サイバー・スパイ	**インフラ**、宇宙、サイバー、軍事／防衛、
9	サイバー・オペレーション	**インフラ**、宇宙、サイバー、社会、行政、軍事／防衛
10	領空侵犯	**軍事**／防衛、社会、政治、外交
11	領海侵入	**軍事**／防衛、社会、政治、外交
12	兵器拡散	**軍事**／防衛
13	軍隊の通常型／準通常型の作戦行動	**軍事**／防衛
14	準軍事組織（傀儡組織）	**軍事**／防衛
15	軍事演習	**軍事**／防衛、外交、政治、社会
16	離散民族の影響工作への利用	**政治**、外交、社会、文化、インテリジェンス、情報
17	文化団体やシンクタンクへの財政支援	**社会**、文化、政治、外交
18	社会的・文化的分裂（民族、宗教、文化）の利用	社会、**文化**
19	社会不安の増長	**インフラ**、社会、経済、政治
20	社会の分極化、リベラル民主主義弱体化のため移民に関する言説を操作	**社会**、文化、政治、法律
21	行政（危機管理を含む）における脆弱性の利用	**行政**、政治、社会

22	汚職の助長と悪用	**行政**、経済、法律、社会
23	法の閾値、行為者特定困難性、未整備部分及び曖昧性の利用	インフラ、サイバー、宇宙、経済、軍事／防衛、文化、社会、行政、**法律**、インテリジェンス、外交、政治、情報
24	法的規制、プロセス、制度、議論の拡大利用	インフラ、サイバー、宇宙、経済、軍事／防衛、文化、社会、行政、**法律**、インテリジェンス、外交、政治、情報
25	インテリジェンス上の準備	**インテリジェンス**、軍事／防衛
26	隠密活動	**インテリジェンス**、軍事／防衛
27	浸透工作	**インテリジェンス**、軍事／防衛
28	外交的制裁	**外交**、政治、経済
29	ボイコット	**外交**、政治、経済
30	大使館及び大使館員の活用	**外交**、政治、インテリジェンス、社会
31	混乱や対立的なナラティブの創出	**社会**、情報、外交
32	国際関係上の取引材料としての移民の利用	**社会**、情報、外交
33	指導者や候補者の信用失墜	**政治**、行政、社会
34	政治的アクターへの支援	**政治**、行政、社会
35	政治家および／または政府への強制・強要	**政治**、行政、法律
36	政治的影響力のための移民の利用	**政治**、社会
37	メディア・コントロール及び干渉	**情報**、インフラ（メディア）、社会、文化
38	偽情報拡散とプロパガンダ	**社会**、情報、政治、サイバー、文化、行政
39	カリキュラムと学術界への影響行使	**社会**、文化
40	電子戦 （GNSS 妨害及びなりすまし）	**宇宙**、サイバー、インフラ、経済、軍事／防衛

出典：**European Commission, & Hybrid CoE,** ***The Landscape of Hybrid Threats: A Conceptual Model Public Version,*** **2021 , pp. 33-35** を元に執筆者作成

別紙 2

フェーズとアクティビティの関係

<table>
<tr><th>時期的フェーズ</th><th>ハイブリッド脅威のアクティビティ</th></tr>
<tr><td>条件形成フェーズ
（priming）</td><td rowspan="3">・撹乱（interference）
＝ハイブリッド脅威のツールを用いて、対象ドメイン内の相手の活動を混乱させて不安定化に向かう下地を作る。
・影響行使（influence）
＝ハイブリッド脅威のツールを用いて、対象ドメインでの相手の活動に何らかの影響を与えて不安定化を図り、作戦を行い易くする。
・作戦実施（operation）
＝ハイブリッド脅威のツールを組み合わせて行使することにより、相手に所望の行動を強要し、目的を達成する。</td></tr>
<tr><td>不安定化フェーズ
（destabilization）</td></tr>
<tr><td>強制フェーズ
（coercion）</td><td>・戦争（war/warfare）
＝軍事戦争の中でハイブリッド脅威のツールを使用し、軍事戦争を有利にする。</td></tr>
</table>

出典：**European Commission, & Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, 2021, p. 13** を元に作成

別紙 3

13 の工作手段の概要

(1)インフラに関連した工作手段

インフラに対する物理的打撃	通信、データ、交通、エネルギー生産、水資源などのインフラに対し物理的破壊工作を行うこと
	例：海底ケーブルの切断
インフラへの依存の構築と利用	工作活動をする側がエネルギー通信、水資源などのインフラを自国に依存させ、影響力を行使するのに利用すること
	例：パイプライン、ダム、海底ケーブル、人工衛星などの資源や通信の供給インフラを供給側がコントロールすることで供給が制限し相手国を混乱に陥らせること

(2)経済に関連した工作手段

経済的依存関係の構築又は利用	貿易などを通じて相手国の自国への依存関係を構築し、影響力を行使すること
	例：相手国の主要産品の輸入、希少資源やサプライ・チェーン上の重要産品の輸出など
外国への直接投資	相手国の民間企業などに直接投資することにより影響力を行使すること
	例：資源・インフラを支配するための投資、経済全般の支配力を高めるための投資
産業スパイ	相手国の企業、研究施設などから産業情報を入手し、産業上の影響力を行使すること
	例：協力者の獲得、技術者の引き抜き、資本関係を通じた技術獲得
相手国経済活動の阻害	相手国の主要産業に必要不可欠な物資等をコントロールして影響力を行使すること
	例：重要な資源・部品等の輸出制限や国際市場コントロールなど
経済的困窮の利用	相手国において経済的に困っている住民を支援することにより影響力を行使すること
	例：雇用状態が悪い地域への産業進出、農産品買い上げ、自国への出稼ぎ奨励

(3)サイバーに関連した工作手段

サイバー・スパイ	サイバー空間内で、サイバー攻撃のための準備を行ったり、軍事情報、産業情報、社会情報などを入手すること
	例：政府、企業等のサーバー等に侵入し、情報を入手すること
サイバー・オペレーション	サイバー空間において、相手国の行動を制限し、自国の利益になるようなサイバー攻撃を行うこと
	例：bot などを使用した偽情報拡散や重要インフラのシステム破壊・混乱及びシステムを通じた物理的破壊

(4) 軍事に関連した工作手段

領空侵犯	軍の有人機又は無人機などにより領空を侵犯し威嚇又は情報活動等を実施すること
	例：日常的な侵犯の継続、大規模演習時の多数機による侵犯
領海進入	軍民を問わず領海、接続水域、EEZ に侵入を繰り返し既成事実化するなどして圧力をかけること
	例：大量の漁船の終結、法執行船の管轄権行使、調査船の活動、軍艦の活動
兵器拡散	相手国又はその周辺国に対する武器輸出などにより影響力を行使すること
	例：相手国への武器輸出で依存関係構築、周辺国への輸出で軍事バランスを有利にすること
軍隊の通常型／準通常型の作戦行動	通常戦力による国境侵犯等の限定攻撃のほか、準通常戦力による隠密の作戦で威嚇し、影響力を行使すること
	例：国境侵犯、砲撃、艦艇攻撃等で威嚇、特殊部隊が潜入し、破壊等で相手国内に不安をつくりだすこと
準軍事組織の利用	相手国内に存在する準軍事組織を代理戦力として利用し、内乱を生起させることなどにより相手国内を不安定にすること
	例：武装している集団の利用、隠密裏に武器を供給し代理手段を武装化すること
軍事演習	各種規模の軍事演習を実施することにより、相手国及びその同盟国をけん制、威嚇すること
	例：各演習、大規模部隊による演習、相手国近傍における演習による経済活動妨害、ミサイル発射、新兵器の試験

(5)文化に関連した工作手段

離散民族の影響工作への利用	相手国に所在している自国又は他国出身の民族を利用して社会不安定化のための工作を実施すること
	例：反政府運動の先導、分離独立運動の実施、偽情報等の拡散、文化的対立の扇動
文化団体やシンクタンクへの財政支援	相手国内の文化団体やシンクタンク等に公に又は隠密裏に資金を提供し影響力を行使すること
	例：直接自国の主張を広める団体に資金提供、資金を通じ間接的に影響を拡大すること
社会文化的分裂の利用	相手国社会に内在する民族、宗教、文化等に起因する国内の文化的対立を利用し社会的分裂を画策すること
	例：民族や宗教上の対立を助長・扇動すること、歴史に起因する対立を掘り起こし、助長すること
カリキュラムと学術界への影響行使	大学教員等学者に浸透し、自国のナラティブ浸透や相手国の文節助長のためカリキュラムを変更すること
	例：学者への資金提供や地位提供等による抱き込み、目立たないようカリキュラムを変更すること

(6)社会に関連した工作手段

社会不安の助長	相手国内の様々な社会的対立や政府に対する不信感を煽ることによって社会不安を助長すること
	例：社会問題を刺激して意図的に対立を煽ることや個別の政策への反対運動を組織化すること
社会の分極化、リベラル民主主義弱体化のため移民に関する言説を操作	相手国社会で移民に関する偏見や不安を生むように意見を操作し、極端な政治的意見を蔓延させて相手国社会を分断すること
	例：移民の不祥事などに関して偽情報を拡散させることや移民を装って社会的対立を扇動すること

(7)行政に関連した工作手段

行政における脆弱性の利用	行政機関の災害、事故等への対応不備などに漬け込み、不信感を助長するとともに政府支持低下を画策すること
	例：災害、事故時のパニック助長や暴動の扇動、デマ拡散による不安や不満を助長すること
汚職の助長と悪用	汚職を煽ることで行政機関への信頼を低下させるとともに、自国に有利なように利用すること
	例：中央・地方行政組織や軍・警察などの汚職を助長、買収による抱き込み工作

(8) 法律に関連した工作手段

法の未整備部分及び適用に関	相手国の法律の欠陥や不備や曖昧性を悪用し、相手国に社会安

する曖昧性の利用	定を助長すること
	例：社会的分裂を煽る内容の訴訟提起、法的犯罪であることが明確でない反社会的行動の扇動により社会不安を助長すること
法規則、制定過程、法制度及び法的論争の利用	相手国政府が様々な事態に対応する際の法の不備、曖昧性、複雑性につけ込み有効な対処を阻害すること
	例：事実認定のための法手続き不備の活用や法執行と武力行使の曖昧性を活用すること

(9) インテリジェンスに関連した工作手段

インテリジェンス上の準備	合法・非合法の手段を用いて、相手国の脆弱性に関する情報を収集し、弱点を分析すること
	例：政治家等のスキャンダル収集、行政機関・軍等の弱点分析
隠密工作	隠密の工作員等による暗殺、破壊活動、事故を起こす、デマを拡散させるなどの活動で社会的影響力を行使すること
	例：真相を偽装した事件等を起こし国家間や社会内の分断を助長すること
浸透	相手国の政府、政党、行政機関、軍、有力企業等に協力者を送り込み又は獲得して影響力を行使すること
	例：自国の工作員を相手国機関へ送り込むこと、相手国内で協力者を獲得すること

(10) 外交に関連した工作手段

外交的制裁	相手国に対し直接外交上の不利益を強いるとともに、他の第３国に対し同様の措置を強要すること
	例：国交断絶、第３国に対して国交断絶を強要すること
ボイコット	相手国が国際機関や国際イベントに参加することに対するボイコットを行い外交的に孤立するよう画策すること
	例：国際会議等からの相手国の締め出し、オリンピック等のイベントをボイコットすること
大使館及び大使館員の活用	大使館等の在外公館及び公館員を取引手段として使用するとともに、本来の外交目的外に悪用すること
	例：大使の召還、公館の閉鎖、相手国館員の追放など
国際関係上の取引材料としての移民問題の利用	外交的な取引材料として移民の流出、送り込み、通過、受け入れ、送還などの措置を利用すること
	国境を越えての移民の送り込み

(11)政治に関連した工作手段

指導者や候補者の信用失墜	相手国の政治指導者やその候補者に関するデマ流布等により信用を失墜させること
	例：スキャンダル等を拡散し、政策失敗に導き、権威を失墜させること
政治的アクターへの支援	自国に有利な政治家や政党への資金面、政策面で支援すること
	例：企業等の迂回手段を用いて政治資金を提供すること
政治家や政府への強制	各種手段を用いて、政治家や政府が自国に有利な政策を取るよう強制すること
	例：相手国経済へアメとムチを用いて強制したり、政治的弱点に付け込んで強制すること
政治的影響力のための移民の利用	移民問題の政治問題化を助長することにより、相手国の政治に影響力を行使すること
	例：移民問題をクローズアップさせるように偽情報や謀略等を活用すること

(12) インフォメーションに関連した工作手段

メディア・コントロール及び干渉	相手国メディアを直接傘下に入れる、もしくは各種手段で影響力を行使し、報道内容に介入すること
	例：メディアの買収、資本関係の強化
偽情報拡散及びプロパガンダ	メディア・SNS・口コミ等を活用して偽情報や悪意のある情報を広範囲に拡散すること
	例：政府不信を生む情報の拡散や自国に都合の良い情報拡散
混乱や対立的ナラティブの創出	相手国内に混乱や対立を生む、もしくは自国支持につながるナラティブを創出し、各種手段で拡散すること
	社会の分裂を促す民族･宗教関連の歴史的ナラティブを創出し、拡散すること

(13) 技術に関連した工作手段

GNSS 妨害やなりすましといった電子戦	妨害電波やなりすまし信号を使用して、衛星経由を含む各種電波の妨害又は乗っ取りで混乱を起こすこと
	例：GPS 信号、他の各種電波への妨害

(14)その他の工作手段

選挙介入	相手国の選挙において自国に都合の良い候補者が当選するよう活動を行うこと
	例：立候補者に関する偽情報の拡散、政治資金の提供
生成 AI の影響	急速に発展する生成 AI の影響は注目しておく必要がある。
	例：画像、音声、動画、などを自動かつ瞬時に生成できるため、偽情報やプロパガンダの拡散が加速

別紙 4

データベースを用いた工作手段ごとの傾向の分析結果

(1) インフラに関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国[55]	その他
インフラに対する物理的打撃	**17**	**11**	**6**	**5**	**4**	**0**	**0**	**0**	**2**	**0**	**3**	**0**	**0**	**0**	**2**	**6**
インフラへの依存の構築又は利用	**5**	**2**	**3**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**

・アクターは主に中国、ロシア、海底ケーブルの切断はアクターが不明なものもあり。

・海底ケーブル切断の工作対象となったところは、アクターと利害関係が対立関係にあるところが多い。

・海底ケーブルの切断はアクターの特定、意図の立証が困難、公海上では国際法取り締まりができないことから、今後も行われる可能性大

(2) 経済に関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
経済的依存関係の構築又は利用	**8**	**4**	**4**	**3**	**0**	**0**	**1**	**0**	**0**	**0**	**3**	**0**	**0**	**0**	**0**	**1**
外国への直接投資	**18**	**16**	**2**	**15**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**12**
産業スパイ	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**
相手国経済活動の阻害	**24**	**15**	**9**	**10**	**0**	**0**	**5**	**0**	**0**	**2**	**1**	**0**	**2**	**1**	**0**	**9**
経済的困窮の利用	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**

・アクターは主として中国である。台湾等に対して直接影響を及ぼすものもあるが、発展途上国等へ行う事例も多い。

・中国経済の状況により影響力は左右されると思われるが当面の間は上記傾向が継続すると考えられる。

(3) サイバーに関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
サイバー・スパイ	**16**	**16**	**0**	**8**	**3**	**3**	**1**	**0**	**1**	**2**	**0**	**0**	**0**	**0**	**0**	**14**
サイバー・オペレーション	**51**	**44**	**7**	**4**	**11**	**0**	**1**	**0**	**28**	**8**	**2**	**13**	**1**	**0**	**5**	**15**

・アクターは主としてロシア、中国であるが、不明なものも多い。

・工作対象は、台湾は件数として低い傾向にあるが、実際の工作活動数（サイバー攻撃）は非常に多い。

・アクターを特定しにくい工作手段であり、今後も多用されると考えられる。

・公開情報と実際のサイバー攻撃の件数の際については、今後の分析の際にも注意すべき。

---

[55] 宇国：ウクライナの略。

(4) 軍事に関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
領空侵犯	**8**	**7**	**1**	**7**	**1**	**0**	**0**	**0**	**0**	**4**	**2**	**1**	**0**	**0**	**0**	**0**
領海侵入	**13**	**13**	**0**	**12**	**0**	**0**	**1**	**0**	**0**	**9**	**1**	**0**	**0**	**1**	**0**	**2**
兵器拡散	**12**	**11**	**1**	**3**	**2**	**2**	**4**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**11**
軍隊の通常型／準通常型の作戦行動	**10**	**4**	**6**	**0**	**0**	**0**	**4**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**4**
準軍事組織（代理勢力）	**9**	**7**	**2**	**7**	**0**	**0**	**0**	**0**	**0**	**1**	**2**	**1**	**1**	**1**	**0**	**1**
軍事演習	**18**	**8**	**10**	**8**	**0**	**0**	**0**	**0**	**0**	**3**	**4**	**0**	**1**	**0**	**0**	**0**

・アクターは中国、対象国が台湾となるものが圧倒的に多い。

・アクターは兵器生産国、高い軍事力保有国が大半を占める。

・アクターは特定しやすいが、アクターの目的、特定のための情報収集が重要と考えられる。

(5) 文化に関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
離散民族の影響工作への利用	**8**	**8**	**0**	**4**	**1**	**0**	**3**	**0**	**0**	**0**	**1**	**2**	**0**	**0**	**0**	**5**
文化団体やシンクタンクへの財政支援	**8**	**8**	**0**	**3**	**0**	**0**	**2**	**2**	**1**	**0**	**0**	**4**	**0**	**0**	**0**	**4**
社会文化的分裂の利用	**4**	**3**	**1**	**3**	**0**	**0**	**0**	**0**	**0**	**2**	**1**	**1**	**0**	**0**	**0**	**0**
カリキュラムと学術界への影響行使	**3**	**3**	**0**	**3**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**1**

・アクターは中国が中心、対象国は日本、米国等の利害関係が対立する国が多い。

・長い時間をかけて工作活動を行っているものと考えられ、特に資金関係の流れが兆候を探知するポイントと思われる。

(6) 社会に関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
社会不安の助長	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
社会の分極化、リベラル民主主義弱体のための移民に関する言説を操作	**6**	**5**	**1**	**0**	**0**	**0**	**0**	**0**	**5**	**0**	**0**	**2**	**0**	**0**	**0**	**3**

・アクターは特定されていない。

・移民問題は住民の不満・不安感をあおりやすく、アクターが特定しにくいことや、アクターが現地住民である場合も考えられることから、工作手段であるか、否か見分けるのは非常に困難。情報収集方法について要検討。

(7) 行政に関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
行政における脆弱性の利用	**2**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**1**
汚職の助長と悪用	**5**	**5**	**0**	**5**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**1**	**0**	**0**		**2**

・中国によるさまざまな国への汚職に関連した工作活動が行われている。

・上記の傾向は今後も継続すると考えられる。

(8) 法律に関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
法の閾値、行為者特定の困難性、未整備部分及び曖昧性の利用	**8**	**7**	**1**	**7**	**0**	**0**	**0**	**0**	**0**	**4**	**1**	**0**	**0**	**0**	**0**	**2**
法規則、制定過程、法制度及び法的議論の利用	**19**	**16**	**3**	**16**	**0**	**0**	**0**	**0**	**0**	**4**	**1**	**0**	**0**	**0**	**0**	**11**

・中国が日本に対して行っているものが中心。国際法と中国の国内法を組み合わせ、独自の主張を展開

・今後も上記活動が予想される。

(9) インテリジェンスに関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
インテリジェンス上の準備	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**
隠密工作	**14**	**13**	**1**	**3**	**3**	**2**	**4**	**0**	**1**	**2**	**1**	**0**	**0**	**0**	**2**	**8**
浸透	**31**	**31**	**0**	**15**	**5**	**2**	**8**	**0**	**1**	**2**	**6**	**6**	**0**	**0**	**1**	**16**

・アクターは中国、ロシア、北朝鮮が中心、対象国は、日本、台湾、米国、ヨーロッパが多数

・特に台湾は事例数（報道数）に比してスパイ件数が圧倒的に大であることから、分析をする際には留意が必要

(10) 外交に関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
外交的制裁	**7**	**5**	**2**	**4**	**0**	**0**	**1**	**0**	**0**	**0**	**2**	**1**	**0**	**0**	**0**	**2**
ボイコット	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**
大使館及び大使館員の活用	**2**	**2**	**0**	**2**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**0**	**0**	**0**	**0**
国際関係上の取引材料として移民問題の利用	**9**	**9**	**0**	**0**	**4**	**0**	**5**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**9**

・アクターは中国、ロシアが中心、対象国は、日本、台湾、米国、ヨーロッパが多数

・アクターは外交力をもった大国。ニュースとして取り上げられやすい。

(11) 政治に関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
指導者や候補者の信用失墜	**2**	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**
政治的アクターへの支援	**6**	**3**	**3**	**3**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**2**
政治家や政府への強制	**7**	**5**	**2**	**1**	**0**	**0**	**4**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**3**
政治的影響力のための移民の利用	**9**	**9**	**0**	**0**	**3**	**0**	**2**	**0**	**4**	**0**	**0**	**1**	**0**	**0**	**0**	**8**

・アクターは中国、ロシアが中心。

・事例数は少ないのは、アクターが隠密裏に活動を行っていることに加え、政府が公にしていない可能性。

(12) インフォメーションに関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
メディア・コントロール及び干渉	**19**	**19**	**0**	**12**	**3**	**1**	**3**	**0**	**0**	**2**	**1**	**2**	**0**	**0**	**1**	**13**
偽情報拡散及びプロパガンダ	**32**	**22**	**10**	**16**	**2**	**1**	**2**	**0**	**1**	**4**	**6**	**4**	**0**	**0**	**0**	**8**
混乱や対立的ナラティブの創出	**8**	**4**	**4**	**3**	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**1**

・アクターは中国、ロシアが中心、対象国は、日本、台湾、米国、ヨーロッパが多数

・生成 AI が活動を助長しており、今後件数の増加が予想される。

(13) 技術に関連した工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシ	北朝	その	非国	不明	日本	台湾	米国	豪国	比国	宇国	その
電子戦（GNSS 妨害及びなりすまし）	**7**	**6**	**1**	**1**	**3**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**6**

・ロシアがアクターとして、ウクライナ侵略で行っているものが中心

・中国は海警船の AIS 信号の変更を実施

・GNSS 妨害は交通機関、金融機関を混乱させるのに効果的であり、活用される可能性大、中国は海警船の AIS 信号の変更も今後継続すると予想される。

(14) その他の工作手段

主ツール	件　数			アクター（事例）						対象国（事例）						
	総数	事例	予測	中国	ロシア	北朝鮮	その他	非国家	不明	日本	台湾	米国	豪国	比国	宇国	その他
選挙介入	**16**	**14**	**2**	**6**	**5**	**0**	**0**	**1**	**2**	**2**	**4**	**3**	**0**	**0**	**0**	**5**
生成 AI に関連した影響工作	**9**	**8**	**7**	**3**	**2**	**0**	**1**	**0**	**2**	**1**	**1**	**2**	**0**	**0**	**0**	**3**

・アクターは中国、ロシアが中心。利害関係国への工作が大半

・生成 AI の利用は今後、増加することが予想される

別紙 5

対台湾・懐柔路線の細部

条件形成フェーズ（懐柔路線）（Taiwan/Coaxing/Priming）

TCP1：インテリジェンス活動

Tool 8（サイバー・スパイ）

・痕跡を残さないようにサイバー進入、必要な時に攻撃に切り替える準備（APT）

Tool 25（インテリジェンス上の準備）

・親中派・反中派の人脈の洗い出し

・台湾経済界内の資本関係等を解明

Tool 27（浸透）

・政党・政府機関・民間企業・軍等への要員の潜入及び協力者の獲得

TCP2：親中政治家の取り込み

Tool 34（政治的アクターへの支援）

・経済支援/政策協調/世論操作

TCP3：親中国派の取り込み

Tool 3（経済的依存関係の構築）

・親中国派を取り込むため経済的な結びつきを強化

Tool 4（外国への直接投資）

・台湾への直接投資を増やすことにより、台湾経済界内での影響力を強化

Tool 37（メディア・コントロール及び干渉）

・台湾メディアを買収し、親中世論を惹起

Tool 17（文化団体やシンクタンクへの財政支援）

・親中的な団体に財政支援し影響力拡大

TCP4：台湾の外交活動の妨害

Tool 28（外交的制裁）

・台湾を国家承認している国家に対して圧力を継続すると同時に、中国と外交関係を有している国が台湾と経済関係等を強化することはむしろ奨励しつつ、各国にとって中台統一が利益となるような方向へ誘導

TCP5：台湾との経済相互依存の強化

●経済的アメとムチ

Tool 3（経済的依存関係の構築）

・金門・馬祖への経済的依存関係を強化しその影響力を拡大する。

・「台湾統一」へのモデル地区、福建省に開設

・経済活動を促進したり制限したり、揺さぶりをかけ、その影響力を拡大

●インフラへの依存

Tool 2（インフラへの依存構築）

・エネルギー供給依存、通信インフラの依存関係を強化しその影響力を拡大する。

TCP6：軍事的恫喝（弱）

Tool 15（軍事演習）

・政権の親中度に合わせて周辺での軍事演習の強度を変化させて反中派をけん制

TCP7：日米への不信感助長

Tool 31（混乱や対立的ナラティブの創出）

・「過去の日本の台湾侵略」に関する中国に都合のよいナラティブの発信

・世界的米中対立の中で、米国は自国のことしか考えていないとのナラティブ発信

Tool 38（偽情報拡散及びプロパガンダ）

「日本は台湾の支援に懐疑的」「米国は台湾を助けない」等の偽情報

不安定化フェーズ（懐柔路線）（Taiwan/Coaxing/Destabilization）

TCD1: 反中勢力の信用失墜

Tool 38（偽情報拡散及びプロパガンダ）

・反中派のスキャンダル等の偽情報の拡散

Tool 26（隠密工作）

・反中派の行動に見せかけた暴動や暗殺の生起

TCD2：台中連携の重要性宣伝

●「平和フレームワーク」の宣伝

Tool 38（偽情報拡散及びプロパガンダ）

・一国二制度より多くの自治権を強調した「平和フレームワーク」を宣伝

Tool 9（サイバー・オペレーション）

・中国のプロパガンダに対する SNS 等での賛意（ボット等による虚偽投稿）拡大

●経済連携強化の強制

Tool 35（政治家や政府への強制）

・台湾との貿易と投資の重要性を再強調し、政治家が親中政策を取るよう強制

TCD3：米国への不信感の助長

Tool 38（偽情報拡散及びプロパガンダ）

・「米国が台湾を支援しないことと引き換えに米・中二国間貿易交渉で合意」したとの偽情報（宣伝）

強制フェーズ（懐柔路線）（Taiwan/Coaxing/Coercion）

TCC1：中国との結びつき強化

●経済的結びつきの制度化

Tool 3（経済的依存関係の構築又は利用）

・親中政権と政府間で公式に両地域の経済を統合する枠組みに合意

TCC2：台湾の情報空間の中国による支配

●ネット空間での情報発信の強化

Tool 9（サイバー・オペレーション）

・台湾のインターネット空間への介入

Tool 38（偽情報拡散及びプロパガンダ）

・ネット空間の安全な利用のためには米国式より中国式が優れているとの言説流布

●メディアの取り込み

Tool 37（メディア・コントロール及び干渉）

・台湾メディアを資本面で支配し、反中的な報道を排除

TCC3：選挙への公然・非公然の介入

Tool 9 サイバー・オペレーション）

・SNS 空間等においてボット等を活用し選挙活動に介入

・選挙システムをハッキングし、結果を操作

Tool 38（偽情報拡散及びプロパガンダ）

・反中勢力が政権を取ると直ちに戦争状態になる等の偽情報を拡散

TCC4：統一を主張する政府樹立

●成立した親中政権を全面的に支援するとともに、反中派の弾圧に協力

Tool 34（政治的アクターへの支援）

・親中政党・政治家への資金援助

Tool 21（行政における脆弱性の利用）

・反中派を弾圧するための警察能力に関し、ノウハウや器材提供等で支援

Tool 24（法規制、制定過程、法制度及び法的議論の利用）

・親中政権成立後ただちに、反中派取り締まりのための法制定を実施

別紙 6

対台湾・強硬路線の細部

条件形成フェーズ（強硬路線）（Taiwan/Hardline/Priming）

THP1：インテリジェンス活動

Tool 8（サイバー・スパイ）

・痕跡を残さないようにサイバー進入、必要な時に攻撃に切り替える準備（APT）

Tool 25（インテリジェンス上の準備）

・台湾軍の脆弱ポイントを探る。

・重要インフラの脆弱ポイントを探る。

Tool 27（浸透）

・軍・警察・台湾当局・政党等への要員の潜入及び協力者の獲得

THP2；政治家への恫喝と信用低下

Tool 33（政治家の信用失墜）

・スキャンダルの暴露。情報操作

Too 35（政治家/政治への強制・強要）

・恐喝と脅迫、選挙への不正介入

THP3：政治的・社会的分断

●統一派・独立派の分断

Tool 37(メディア・コントロール及び干渉)

・海外のメディア企業や出版社を買収、広告や投資を通じて影響力を行使

Tool 31（混乱や対立的ナラティブの創出）

・統一派、独立派それぞれのナラティブを強化することにより相互に妥協できない雰囲気を醸成

Too 18（社会文化的分裂（民族・宗教・文化）の利用）

・大陸との宗教的つながりの利用（両岸にある媽祖信仰を通じた影響行使）

●本省・外省人の分断

Tool 18（社会的・文化的分裂の利用）

・歴史的経緯から来る社会的優位性（差別）に関する矛盾を利用し国内を混乱

THP4：国際的組織からのボイコット

Tool 28（外交的制裁）

・台湾を国家承認している国家や親台湾的な国家との外交関係を妨害（台湾の孤立化）

Tool 29（ボイコット）

・台湾を国際的組織、国際的イベントからのボイコット

THP5：台湾の経済的活動の妨害

Tool 6（相手国経済活動の妨害）

・政府公的機関による輸出入規制

・経済協力枠組み協定の一時停止
・台湾の多国籍企業に対する広範な制限

THP6：軍事的恫喝（強）

Tool 15（軍事演習）
・台湾周辺での軍事演習（接続水域接近、通過）
・台湾の上空および周辺で長距離ミサイルの複数のテスト

Tool 10（領空侵犯）
・気球、無人、有人機による中間線等の越境

Tool 11(領海侵入（EEZ 含む）)
・金門・馬祖周辺における漁船及び海警の活動強化
・東沙諸島・太平島周辺における海警及び海軍の行動

不安定化フェーズ（強硬路線）（Taiwan/Hardline/Destabilization）

THD1：政府の行政能力不信助長

●民間船舶航行妨害

Tool 11（領海侵犯）
・金門、馬祖付近航行船舶への妨害

●領空侵犯

Tool 10（領空侵犯）
・金門、馬祖上空へドローンの大群を飛来させる。

THD2：社会不安、戦争への不安の助長

●銀行の障害

Tool 9（サイバー・オペレーション）
・DDoS 攻撃による銀行の Web サイト閲覧不能

Tool 38（偽情報拡散及びプロパガンダ）
・「〇〇銀行取引不能」との偽情報の拡散

●医療障害

Tool 9（サイバー・オペレーション）
・医療機関電子カルテ障害による、医療不安、障害

Tool 38（偽情報拡散）
・多くの医療機関の障害との偽情報の拡散

●危機を煽る

Tool 38（偽情報拡散及びプロパガンダ）
・台湾当局の職員が個人的な脱出計画を立てているとの噂の流布

Tool 15（軍事演習）
・台湾周辺海域へのミサイル発射演習

Tool 19(社会不安の助長)
・犯罪組織を利用して暴力犯罪を増大させる等により社会不安を助長

THD3：台・米・日の連携障害

●海底電線切断

Tool 1（インフラに対する物理的打撃）

・日米台間の情報共有を妨害するための漁船等を使用した海底電線の切断

強制フェーズ（強硬路線）（Taiwan/Hardline/Coercion）

THC1：社会、経済活動の混乱

●重要インフラ障害

Tool 9（サイバー・オペレーション）

・航空管制、鉄道、電力、ガス、水道、物流、石油のインフラにかかわる障害

●軍事演習による経済活動妨害

Tool 15（軍事演習）

・台湾接続水域内での中ロ共同演習

・船舶検査の法的根拠を制定

・太平島に対する接近封鎖

●経済活動の妨害

Tool 6（相手国経済活動の妨害）

・輸出入大幅制限、ビザ発給禁止、

・台湾の貨物機を中国に強制着陸

THC2：台湾の情報発信の孤立化

●通信ネットワークの障害

Too l1（物理的打撃）

・世界との情報発信を妨害するために、海底電線を切断、工作員による引揚局舎隠密破壊

Tool 9（サイバー・オペレーション）

・データーセンターへのサイバー攻撃

・通信ネットワークへのサイバー攻撃

Tool 40（電子戦）

・衛星回線への電子妨害

THC3：内乱を作為

Tool 14（準軍事組織（代理勢力））

・台湾の親中代理勢力が武力蜂起し、内乱状態が生起

THC4：限定的軍事介入

●軍隊の内政への介入

Tool 15（軍隊の通常型/準通常型の作戦行動）

・親中勢力（政権）からの要請を受けて、軍事支援実施、状況により部隊を派遣

●島嶼部へのミサイル攻撃

Tool 15（軍隊の通常型/準通常型の作戦行動）

・米国の出方をチエックするための島嶼部（彭佳嶼等）へのミサイル発射

別紙７

対日本・懐柔路線時の細部

条件形成フェーズ（日/台の離反）（Japan/Coaxing/Priming）

JCP1：インテリジェンス活動

Tool 8（サイバー・スパイ）

・痕跡を残さないようにサイバー進入、必要な時に攻撃に切り替える準備（APT）

Tool 25（インテリジェンス上の準備）

・日台間の分断に繋がる事象を探る。

・重要インフラの脆弱ポイントを探る。

Tool 27（浸透）

・政府機関、政党、経済団体等に要員の潜入及び協力者の獲得

JCP2：反中派の弱化と親中派の育成

Tool 38（偽情報拡散及びプロパガンダ）

・台湾内の反中派は米から資金を得ており、多数は統一を望んでいる等の偽情報を拡散

Tool 35（政治家や政府への強制）

・親台湾の政治家へ各種圧力をかける。

JCP3：経済を含めた対日強硬策

Tool 3（経済的依存関係の構築又は利用）

・アジア経済における中国主導を強化し、日本とアジア諸国間の経済関係を妨害

Tool 38（偽情報拡散及びプロパガンダ）

・福島処理水問題への強硬姿勢崩さず

Tool 11（領海侵入）

・台湾を巻き込んで尖閣諸島情勢を尖鋭化

JCP4：南西諸島近海、軍事演習での威嚇

Tool 15（軍事演習）

・南西諸島近海で演習を活発化して威嚇

Tool 38（偽情報拡散及びプロパガンダ）

・日本による南西諸島の軍事化を非難

JCP5：中台と沖縄一体とのナラティブ発信

Tool 38（混乱や対立的ナラティブの創出）

・中国・台湾・沖縄は歴史的に一体であり、一体であってこそ繁栄するとのナラティブを拡散

不安定化フェーズ（日/台の離反）（Japan/Coaxing /Destabilization）

JCD2：日台連携強化を阻む工作

●台湾経済からの日米の締め出し

Tool 6（相手国経済活動の妨害）

・台湾及び日米企業に圧力をかけて輸出入を規制

・台湾の多国籍企業に対する広範な制限

●台中の経済連携強化を宣伝

Tool 38（偽情報拡散及びプロパガンダ）

・台湾との貿易と投資を再強調する

・一国二制度より多くの自治権を強調した「平和フレームワーク」を宣伝

JCD3：日台の意思疎通の妨害

●日台の通信障害

Tool 1（インフラに対する物理的打撃）

・日台間の情報共有を妨害するための漁船等を使用した海底電線の切断

●尖閣諸島情勢を巡る日本の海警行動誘発

Tool 24（法規則、制定過程、法制度及び法的議論の利用）

・尖閣の主権は台湾にあるとの台湾当局による独自の主張に基づく視点から、日本の海警行動を契機に台湾の反日派の世論を惹起させ日台を離反させる。

●台湾は日本に期待していないとの風評

Tool 38（偽情報拡散及びプロパガンダ）

・台湾は日本に期待していないとの風評の流布

強制フェーズ（日/台の離反）（Japan/Coaxing/Coercion）

JCC1：日本と台湾民主化勢力の分断工作

Tool 38（偽情報拡散及びプロパガンダ）

・「台湾は民主的に統一に向かう」との偽情報拡散

・反中勢力に関するスキャンダル偽情報拡散

Tool 3（経済的依存関係の構築又は利用）

・統一の既成事実を認めるならば経済優遇、認めないならば制裁

Tool 9（サイバー・オペレーション）

・SNS 上でボット等により台湾内の反日意識、日本内の反台湾意識を煽る論調拡散

JCC2：統一に賛成の世論形成

Tool 38（偽情報拡散及びプロパガンダ）

・国際的にも統一容認が大勢との偽情報拡散

別紙 8

対日本・強硬路線時の細部

条件形成フェーズ（日/米離反）（Japan/Hardline/Priming）

JHP1：インテリジェンス活動

Tool 8（サイバー・スパイ）

・痕跡を残さないようにサイバー進入、必要な時に攻撃に切り替える準備（APT）

Tool 25（インテリジェンス上の準備）

・自衛隊、在日米軍の脆弱ポイントを探る。

・重要インフラの脆弱ポイントを探る。

Tool 27（浸透）

・政府機関、政党、経済団体等に要員の潜入及び協力者の獲得

JHP2：日本の安全保障政策への干渉

Tool 31（混乱や対立的ナラティブの創出）

・日米同盟は、日本を戦争に巻き込むだけで安全に寄与しないとのナラティブ流布

Tool 38（偽情報拡散及びプロパガンダ）

・米国は中台紛争に介入しない決定をした、台湾は中国に抵抗しない等の偽情報を流布

JHP3：対米強硬の反面で対日宥和工作

Tool 3（経済的依存関係の構築又は利用）

・経済的な見返りとともに外交面で秋波

Tool 11（領海侵入）

・尖閣諸島情勢での態度軟化（例：中国漁船の操業の規制）

JHP4：日本周辺海域での軍事演習

Tool 15（軍事演習）

・日本に対し直接脅威を与えるような演習を減らしつつ、周辺海域での米軍部隊に対して挑発的な演習を実施し、日本国民に不安感を醸成

JHP5：沖縄を巡る世論の分断

●米軍への不信感・不安感助長

Tool 37（メディア・コントロール）

・米軍による事件、事故に関連して、バイアスをかけた発信

Tool 38（偽情報拡散及びプロパガンダ）

・米軍人による犯罪等の偽情報を拡散

Tool 9（サイバー・オペレーション）

・SNS 上でボット等により、本土での反沖縄、沖縄で反本土の意見拡散

●沖縄と中国の歴史的つながりの強調

Tool 31（混乱や対立的ナラティブの創出）

・中国は歴史的に沖縄に好意的であり、むしろ沖縄は日本に虐げられてきたとのナラティ

ブを拡散
・沖縄戦に関する旧日本政府及び米国政府の非をことさらに強調

不安定化フェーズ（日/米離反）（Japan/Hardline/Destabilization）

JHD1：政府の行政能力不信助長

●社会機能障害（限定的）による社会不安から政府不信助長

＜銀行の障害＞

Tool 9（サイバー・オペレーション）

・DDoS 攻撃による銀行の Web サイト閲覧不能

Tool 38（偽情報拡散及びプロパガンダ）

・「〇〇銀行取引不能」との偽情報の拡散

＜医療障害＞

Tool 9（サイバー・オペレーション）

・医療機関カルテ障害による、医療不安、障害

Tool 38（偽情報拡散及びプロパガンダ）

・医療機関の障害との偽情報の拡散

●民間船舶保護に関し政府不信助長

Tool 11（領海侵入（EEZ 含む））

・大量の漁船の EEZ 侵入等により、日本国内の政府不信を助長

Tool 38（偽情報拡散及びプロパガンダ）

・海保への不信を煽るためのフェイク画像等偽情報の拡散

Tool 24（法規制、制定過程、法制度及び法的議論の利用）

・法執行と軍事活動の曖昧性の利用

JHD2：日米同盟のリスクを喚起

●経済面での日中関係強化

Tool 3（経済依存関係の構築又は利用）

・輸入や投資に関して日本を優遇し、日本企業との連携を強化

●日本が戦争に巻き込まれるリスク

Tool 15（軍事演習）

・米軍基地への攻撃を模擬したミサイル発射や航空攻撃の演習を実施し、戦争のリスクを宣伝

●米中紛争のリスク

Tool 15（軍事演習）

・第二列島戦越えのミサイル発射等で中国は対米戦争を厭わないことを示し、日米同盟のリスクを日本国民に浸透

JHD3：日米の意思疎通の妨害

●日米の通信障害

Tool 1（インフラに対する物理的打撃）

・日米間の情報共有を妨害するために、漁船等を使用して海底電線を切断

強制フェーズ（日/米離反）（Japan/Hardline/Coercion)

JHC1：日米の分断工作

●日米の情報交換への妨害

Tool 1（インフラに対する物理的打撃）

・通信障害（海底電線、衛星通信）により、機微な日米の情報交換に障害を起こさせる。

Tool 40（電子戦）

・日米間に齟齬を起こさせるための、なりすまし通信等の利用

●自衛隊、在日米軍基地作戦能力の妨害

・日本の重要インフラ（電力、ガス、水道等）へのサイバー攻撃により、それに依存する自衛隊、在日米軍の作戦能力を妨害する。

Tool 38（偽情報拡散及びプロパガンダ）

・偽情報により基地周辺住民、在日米軍家族を不安に陥れる。

JHC2：台湾への不介入の世論形成

Tool 38（偽情報拡散及びプロパガンダ）

・「台湾で統一派が圧倒的優勢」の偽情報拡散

JHC3：「重要影響事態」等認定の遅延

Tool 38（偽情報拡散及びプロパガンダ）

・「重要影響事態」等の認定は中国に対する戦争行為であるとのプロバガンダ

別紙 9

中国による日本へのハイブリッド戦の手段と日本のドメインの関係

目標区分	ツール	標的とされる日本のドメイン												
		外交	政治	文化	社会	法律	軍事・防衛	宇宙	行政	インフラ	経済	インテリジェンス	インフォメーション	サイバー
JHP1 インテリジェンス活動	Tool 8（サイバースパイ）	○	○				○			○	○	○		○
	Tool 25（インテリジェンス準備）	○	○				○			○	○	○		
	Tool 27（浸透）	○	○				○				○	○		
JHP2 日本の安全保障政策への干渉	Tool 31（混乱対立ナラティブ創出）	○	○	○	○	○	○						○	
	Tool 38（偽情報拡散プロパガンダ）	○	○		○		○						○	
JHP3 対米強硬の反面で対日宥和工作	Tool 3（経済的依存関係構築利用）	○	○								○			
	Tool 11（領海侵入）	○	○				○		○					
JHP4 日本周辺海域での軍事演習	Tool 15（軍事演習）	○	○		○		○						○	
JHP5 沖縄を巡る世論の分断	Tool 37（メディア・コントロール）				○								○	
	Tool 38（偽情報拡散プロパガンダ）			○	○								○	
	Tool 9（サイバー・オペレーション）				○								○	○
	Tool 31（混乱対立ナラティブ創出）		○	○	○								○	
JHD1 政府の行政能力不信助長	Tool 9（サイバー・オペレーション）			○	○				○	○	○			○
	Tool 38（偽情報拡散プロパガンダ）			○	○				○	○	○			
	Tool 11（領海侵入（EEZ含む））		○		○		○		○					
	Tool 24（法制度法的議論の利用）		○			○			○					
JHD2 日米同盟のリスクを喚起	Tool 3（経済依存関係の構築利用）	○	○								○		○	
	Tool 15（軍事演習）	○	○		○		○						○	
JHD3 日米の意思疎通の妨害	Tool 1（インフラへの物理的打撃）	○						○		○		○		
JHC1 日米の分断工作	Tool 1（インフラへの物理的打撃）	○					○	○		○		○		
	Tool 40（電子戦）						○	○				○		
	Tool 38（偽情報拡散プロパガンダ）		○		○		○						○	
JHC2 台湾への不介入の世論形成	Tool 38（偽情報拡散プロパガンダ）	○	○		○								○	
JHC3 「重要影響事態」等認定の遅延	Tool 38（偽情報拡散プロパガンダ）		○		○	○	○						○	
JCP1 インテリジェンス活動	Tool 8（サイバースパイ）	○	○								○	○		○
	Tool 25（インテリジェンス準備）	○	○								○	○		
	Tool 27（浸透）	○	○								○	○		
JCP2 反中派の弱化と親中派の育成	Tool 38（偽情報拡散プロパガンダ）	○	○		○								○	
	Tool 35（政治家や政府への強制）		○						○					
JCP3 経済を含めた対日強硬策	Tool3（経済的依存関係の構築利用）	○	○								○			
	Tool38（偽情報拡散プロパガンダ）	○			○								○	
	Tool11（領海侵入）	○	○		○		○						○	
JCP4 南西諸島近海、軍事演習での威嚇	Tool 15（軍事演習）	○	○		○		○						○	
	Tool 38（偽情報拡散プロパガンダ）	○	○		○								○	
JCP5 中台と沖縄一体とのナラティブ発信	Tool 38（混乱対立ナラティブ創出）			○	○								○	
JCD2 日台連携強化を 阻む工作	Too l6（ 相手国経済活動の阻害）	○	○								○			
	Tool 38（偽情報拡散プロパガンダ）	○	○		○								○	
JCD3 日台の意思疎通の妨害	Tool 1（インフラへの物理的打撃）	○						○		○		○		
	Tool 24(法制度法的議論の利用)	○	○			○	○		○					
	Tool 38（偽情報拡散プロパガンダ）	○	○		○								○	
JCC1 日本と台湾民主化勢力の分断工作	Tool 38（偽情報拡散プロパガンダ）	○	○		○								○	
	Tool 3（経済的依存関係構築利用）	○	○								○			
	Tool 9（サイバー・オペレーション）	○	○	○	○								○	○
JCC2 統一に賛成の世論	Tool 38（偽情報拡散プロパガンダ）	○	○		○								○	

出典：海洋安全保障研究委員会作成

(注) 表中で、同じツールであっても標的ドメインが異なるのは、フェーズや目標によってツールの使い方が異なり、標的ドメインが変わって来るためである。

海洋安全保障研究委員会

（委員長）	齋藤　　隆	元統合幕僚長
	福本　　出	元海上自衛隊幹部学校長
	徳地　秀士	中曽根平和研究所研究顧問、 平和・安全保障研究所理事長
	平田　英俊	元航空自衛隊航空教育集団司令官
	松村　五郎	元陸上自衛隊東北方面総監
	中村　　進	慶応義塾大学 SFC 研究所上席所員
	佐藤　考一	桜美林大学教授
	村上　政俊	皇學館大学准教授
	山本　勝也	笹川平和財団主任研究員
	相澤　李帆	防衛研究所研究員
	山本ﾏｸｼﾐﾘｱﾝ拓馬	
	川嶋　隆志	防衛研究所所員
	高畠　　太	中曽根平和研主任研究員
	安江　真理子	中曽根平和研主任研究員