防衛研究所 National Institute for Defense Studies
NIDSコメンタリー
第 403 号　2025 年 10 月 14 日

ハイブリッド戦における工作手段の分類と特徴

－欧州ハイブリッド脅威対策センターのコンセプト・モデルに基づく分析－

戦史研究センター安全保障政策史研究室所員　川嶋　隆志

はじめに

2022 年に開始されたロシアによるウクライナ侵攻は、単なる軍事的衝突にとどまらず、情報戦、経済戦、サイバー戦など多様な手段を組み合わせた「ハイブリッド戦」を通じ、対象国家の政治的・社会的基盤を戦略的に動揺させる手法の有効性及びこれらへの対応の重要性を国際社会に強く印象付けた。

日本周辺においても、中国が台湾統一を目指し、複合的な工作活動を展開している。これらの活動は、情報操作、経済的影響力の行使、技術的優位の確保、文化的浸透など多岐にわたり、ハイブリッド戦の典型的な特徴を備えている。

ハイブリッド戦は軍事的手段・非軍事的手段を組み合わせることで、相手国の脆弱性を突き、社会的混乱や政策決定の妨害を企図するものである。その手法は年々複雑化・高度化し、その影響は一般市民個人にまでも及ぶ。したがって、ハイブリッド戦の実態を体系的に分析・理解することは、安全保障上の喫緊の課題である。

本稿では、欧州ハイブリッド脅威対策センター（European Centre of Excellence for Countering Hybrid Threats）が提示するハイブリッド戦において使用され得る 40 の工作手段[1]を、国力の構成要素に基づき 13 のグループに分類し、それぞれの特徴と代表的事例を公開情報に基づいて整理・分析する。その目的は、複雑化・巧妙化するハイブリッド戦の工作手段を体系的に整理することで、政策立案者や安全保障関係者のみならず、一般市民に対してもその脅威の実態を理解し、把握しやすくすることにある。

なお、本稿におけるハイブリッド戦の各工作手段に関する記述は、筆者による独自の分析に基づいている。

1．インフラを利用した工作手段

欧州ハイブリッド脅威対策センターが作成したハイブリッド脅威分析のためのコンセプト・モデルでは、「インフラに対する物理的打撃」と「インフラへの依存の構築と利用」の 2 つの工作手段が挙げられている。

・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、水資源などの社会基盤を構成する重要なインフラに対し物理的破壊工作を行うことで、国家の経済・社会活動に直接的な打撃を与える手法である。

・インフラへの依存の構築と利用

工作主体(アクター)がエネルギーや通信、水資源などの国家・社会機能を維持する上で不可欠なインフラを依存する状況を対象国に形成し、その依存関係を利用して影響を行使する手法である。具体的には、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制御することで、相手国の混乱を誘発することが挙げられる。

（1）特徴

重要インフラは国民生活や経済活動の基盤であるため、影響工作によってその機能が停止または低下すると、社会に深刻な混乱をもたらす。特にハイブリッド戦においては、SNS やメディアを通じた偽情報の拡散などを併用することで国民の不安を煽り、工作手段による影響を誇大化し、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生むのが特徴である。

（2）代表的事例

・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[2]。

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）に及ぶ海底ケーブルが張り巡らされている[3]。

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難しい。

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[4]、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[5]。

2．経済を利用した工作手段

コンセプト・モデルでは、「経済的依存関係の構築又は利用」「外国への直接投資」「産業スパイ」「相手国経済活動の阻害」「経済的困窮の利用」の 5 つの工作手段が挙げられている。

・経済的依存関係の構築または利用

アクターが貿易や資源供給を通じて対象国の自国に対する依存関係を形成し、それを通じて影響力を行使する手法である。主要産品の輸入や、希少資源・サプライチェーン上の重要品目の輸出などが該当する。

・外国への直接投資

アクターが対象国の民間企業やインフラに対して資本を投入することで、経済的影響力を獲得・拡大する手段である。資源支配や経済構造への介入を目的とする場合が多い。

・産業スパイ

対象国の企業や研究機関から技術・産業情報を不正に取得し、自国の産業競争力を高めるとともに、相手国の技術的優位を低下させることを狙うものである。協力者の獲得、技術者の引き抜き、資本関係を通じた技術移転などが含まれる。

・相手国経済活動の阻害

アクターが対象国の主要産業に不可欠な物資や部品の供給を制限することで、経済的混乱を引き起こす手法である。輸出規制や国際市場の操作などが典型例である。

・経済的困窮の利用

アクターが対象国の経済的弱者層に対して有形・無形の支援を行うことで、親近感や依存関係を形成し、影響力を行使する方法である。雇用の創出、農産品の買い上げ、出稼ぎの奨励などが挙げられる。

（1）特徴

経済を利用した工作手段は、対象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及ぼす。特にハイブリッド戦においては、フェイクニュースや SNS を通じた情報操作を通じて、国民生活に直結する様々な経済問題は政府の怠慢や機能不全によるものだという言説を拡散することで国民の不信感を煽り、政府への信頼を揺るがす効果を持つ。逆に、経済的恩恵がアクターからの経済支援や貿易関係によってもたらされており、対象国にとってアクターとの友好関係は不可欠であるという世論を普及することで、アクターにとって宥和的な政権を樹立することもあり得る。この様に、経済的手段は武力を伴わないため表面的には平和的に見えるが、実質的には戦略的圧力として機能するため、ハイブリッド戦の極めて重要な手段の一つである。

（2）代表的事例

2022 年のロシアによるウクライナ侵攻の際、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[6]。この状況は、欧州各国にとってエネルギー確保と対ロシア制裁という 2 つの重要課題の間でジレンマを生むこととなった[7]。

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[8]。

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[9]。

3．サイバー空間を利用した工作手段

コンセプト・モデルでは、「サイバー・スパイ」と「サイバー・オペレーション」の 2 つが示されている。

・サイバー・スパイ

サイバー空間において、軍事情報、産業情報、社会情報などを収集するために、サーバー等へ侵入する行為を指す。これには、サイバー攻撃の準備段階としての情報収集も含まれる。

・サイバー・オペレーション

サイバー空間において対象国の行動を制限し、自国の利益を促進するために行われる攻撃的手段である。破壊型攻撃、妨害型攻撃、システムへの侵入など多様な手法が含まれる。bot を用いた偽情報の拡散、重要インフラのシステム破壊や混乱、さらにはシステムを通じた物理的破壊などが典型例である。

（1）特徴

サイバー空間を利用した工作手段は、活動主体が国家か非国家主体かを特定しにくいという特徴を有する。国家関与の否定が容易であり、また隠密性が高いため、工作活動の開始時期や実態の把握が困難である。

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、他の工作手段に対する探知・防御能力を封じることで作戦遂行を円滑化するため、複合攻撃における初期段階から活用されることが多い。

（2）代表的事例

2022 年のロシアによるウクライナ侵攻の際、ロシアは侵攻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[10]。

4．軍事を利用した工作手段

コンセプト・モデルでは、「領空侵犯」「領海侵入」「兵器拡散」「軍隊の通常型／準通常型の作戦行動」「準軍事組織」「軍事演習」の 6 つが挙げられている。

・領空侵犯

軍用機や無人機による相手国領空への侵入を通じて、威嚇や情報収集を行う手段である。日常的な侵犯の継続や、大規模演習時の多数機による侵入などが含まれる。

・領海侵入

軍艦や漁船、調査船などが相手国の領海、接続水域、排他的経済水域（EEZ）に侵入し、既成事実化を図ることで圧力をかける手法である。

・兵器拡散

対象国またはその周辺国に対して武器を輸出することで、軍事的依存関係を構築したり、地域の軍事バランスを変化させることを目的とする。

・軍隊による通常型／準通常型の作戦行動

通常戦力による限定的な攻撃や、特殊部隊などによる隠密作戦を通じて、相手国に威嚇や不安を与える手段である。

・準軍事組織の活用

アクターが対象国内に存在する武装集団を代理勢力として利用し、内乱や社会不安を引き起こすことで、国家の統治能力を低下させる方法である。

・軍事演習

各種規模の演習を相手国周辺で実施することで、威嚇やけん制を行う手段である。演習に伴うミサイル発射、新兵器の試験、経済活動への妨害なども含まれる。

（1）特徴

軍事的手段は、相手国に対して直接的な威圧感を与えるとともに、国民や政府に心理的圧力を加える効果を持つ。典型的なものとして、国境付近や係争地域での軍事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、軍事行動がサイバー攻撃や情報操作と連動して用いられることが多く、例えば通信システムを麻痺させた後に軍事力を展開する、演習と同時に偽情報を流布して世論を操作する、あるいは国際法上の曖昧性を利用して軍事行動を正当化するなど、複合的な戦術が展開される。

（2）代表的事例

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[11]、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[12]、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[13]。

5．文化を利用した工作手段

コンセプト・モデルでは、「離散民族の影響工作への利用」「文化団体やシンクタンクへの財政支援」「社会文化的分裂の利用」「カリキュラムと学術界への影響行使」の 4 つが挙げられている。

・離散民族の影響工作への利用

アクターが対象国に居住する自国または第三国出身の民族集団を活用し、反政府運動や分離独立運動、偽情報の拡散、文化的対立の扇動などを通じて社会の不安定化を図る手法である。

・文化団体やシンクタンクへの財政支援

アクターが対象国内の文化団体や研究機関に対して公然または秘密裏に資金を提供し、自国の主張や価値観の浸透を促進する手段である。資金提供などの直接的な支援に加え、アクター国内でのイベント実施その他の活動に対する便宜の提供などといった間接的な影響力の拡大も含まれる。

・社会文化的分裂の利用

アクターが対象国社会に内在する民族、宗教、文化的対立を助長・扇動することで、社会的分裂を引き起こす工作である。歴史的な対立や差別構造を再活性化させることも含まれる。

・カリキュラムと学術界への影響行使

大学教員や研究者に対する資金提供や地位の付与を通じて、アクターのナラティブを教育・研究に浸透させる手法である。教育内容の改変や学術的議論の誘導を目的とする。

（1）特徴

文化を利用した工作手段は、国民のアイデンティティや価値観に直接作用するため、長期的かつ深層的な影響力を持つ。社会の分裂、世論の形成、アイデンティティの変容などを通じて、国家の統治基盤を

揺るがす可能性がある。

また、文化的手段は目に見えにくく、抵抗されにくいという特性を持つ。映画、音楽、文学などのコンテンツを通じて特定の価値観や歴史観を広めることで、相手国の国民の認識に影響を与えることが可能である。ハイブリッド戦においては、こうした文化的浸透が情報操作や心理戦と連動し、戦略的な効果を発揮する。

（2）代表的事例

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[14]。

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[15]。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[16]、若年層の文化的同化が進められている。

6．社会を利用した工作手段

コンセプト・モデルでは、「社会不安の助長」「社会の分極化及び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」の 2 つが挙げられている。

・社会不安の助長

アクターが対象国内に存在する社会的対立や政府への不信感を煽ることで、社会不安を助長する手法である。社会問題を刺激して意図的に対立を煽ることや、個別政策への反対運動を組織化することなどが含まれる。

・社会の分極化及び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

アクターが対象国内で移民に関する偏見や不満を生むように言説を操作し、極端な政治的意見を蔓延させて、対象国社会を分断するものである。

（1）特徴

「社会を利用した工作手段」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拡張す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 による世論操作を多用することで社会の分断や不満を助長し、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。

（2）「社会を利用した工作手段」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拡張し、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[17]。

7．行政を利用した工作手段

コンセプト・モデルでは、「行政における脆弱性の利用」「汚職の助長と悪用」の 2 つが挙げられている。

・行政における脆弱性の利用

災害や事故等に対する行政機関の対応不備を利用し、住民の不信感を助長することで政府支持の低下を図る。具体的には、災害時のパニックの助長、暴動の扇動、偽情報の拡散などが含まれる。

・汚職の助長と悪用

行政機関における汚職を誘発することで信頼性を低下させ、自国に有利な状況を構築する。中央・地方行政組織、軍・警察などに対する買収や抱き込み工作が典型例である。

（1）特徴

行政を利用した工作手段は、行政機関に対する住民の不満や不信感を煽ることで、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含まれる。

汚職は発覚時のインパクトを大きくするためにある程度長期間にわたって継続する必要があるため、隠密に行われると考えられる。

特にハイブリッド戦においては、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 等を活用することで不安や不満を刺激しやすく、行政機関を混乱させる効果が高い。

（2）代表的事例

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[18]、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．法律を利用した工作手段

コンセプト・モデルでは、「法の未整備部分及び適用に関する曖昧性の利用」「法規則、法手続き、法的機関及び法的論争の利用」の 2 類型が示されている。

・法の曖昧性・未整備の利用

アクターが国際法や対象国の法制度における欠陥や曖昧性を悪用し、自国に有利な解釈や行動を取る。具体的には、海域の境界未確定を利用した海域の実効支配や法解釈の拡張などが含まれる。

・法規則・手続き・機関及び法的論争の利用

アクターが国際法をはじめとする法制度や裁判所などを戦略的に利用して、対象国の行動を制限または非難する。法的手続きの乱用、国際裁判所への提起、法的論争の操作などが典型である。

（1）特徴

法律を利用した工作手段は、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、国際世論の操作を図るとともに、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、他の手段との連携が見られる。

（2）代表的事例

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、曖昧な適用海域や武器使用権限などの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[19]。この措置自体は必ずしも国際法違反とは言えないが、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。

9．インテリジェンスを利用した工作手段

コンセプト・モデルでは、「インテリジェンス上の準備」「隠密工作」「浸透」の 3 つが挙げられている。

・インテリジェンス上の準備

合法・非合法の手段を用いて、対象国の脆弱性に関する情報を収集し、弱点を分析する。政治家等のスキャンダル収集、行政機関・軍等の脆弱性分析などがある。

・隠密工作

暗殺、破壊活動、事故の偽装、デマの拡散などを通じて社会的影響力を行使する。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がこれにあたる。

・浸透

対象国の政府、政党、行政機関、軍、有力企業等に協力者を送り込み、または獲得して影響力を行使する。

（1）特徴

インテリジェンスを利用した工作手段は、国家の意図を達成するために秘密裏に実施されるため活動の兆候を察知することが非常に困難であり、仮に発覚しても国家が関与していないと主張されることが

一般的である。

この手段の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。

ハイブリッド戦では、工作員による偽情報の拡散、暴動支援、重要施設へのマルウェア設置などの手段との連携が考えられる。

（2）代表的事例

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[20]、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[21]。

10. 外交を利用した工作手段

コンセプト・モデルでは、「外交的制裁」「ボイコット」「大使館及び大使館員の活用」「移民問題の外交的利用」の 4 つが挙げられている。

・外交的制裁

対象国に対して直接的な外交上の不利益を与えるとともに、第三国にも同様の措置を強要する。国交断絶や第三国への外交圧力が典型例である。

・ボイコット

対象国の国際機関や国際イベントへの参加を妨害し、外交的孤立を図る。国際会議からの排除や国際スポーツイベントのボイコットなどが含まれる。

・大使館及び大使館員の活用

在外公館や外交官を本来の目的以外に利用し、取引材料として活用する。大使の召還、公館の閉鎖、相手国外交官の追放などが挙げられる。

・移民問題の外交的利用

移民の流出・受け入れ・送還などを外交交渉の材料として活用し、対象国に圧力を加えるものである。

（1）特徴

外交を利用した工作手段は、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・経済は、国家の国際的影響力を支える三本柱であり、ハイブリッド戦においてはこれらが相互に連携して機能する。

特に外交手段を通じた影響工作は、経済援助や軍事協力と組み合わせることで対象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の一翼を担い、国際世論の形成に寄与する。

（2）代表的事例

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。昨年からの傾向として、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[22]。

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、台湾が外交関係を有する国は 12 か国に減少した[23]。

11. 政治を利用した工作手段

コンセプト・モデルでは、「指導者や候補者の信用失墜」「政治的アクターへの支援」「政治家や政府への強制」「移民問題の政治的利用」の 4 つが示されている。

・指導者や候補者の信用失墜

アクターが対象国の政治指導者や候補者に関するデマやスキャンダルを拡散し、権威を失墜させることを指す。

・政治的アクターへの支援

アクターが対象国において自国に有利な政治家や政党に対して資金・政策面で支援を行うことである。企業等を通じた迂回的な資金提供が含まれる。

・政治家や政府への強制

アクターが対象国に対し経済的圧力や政治的弱点を利用して、相手国政府に自国に有利な政策を取らせるものである。

・移民問題の政治的利用

アクターが偽情報や謀略を用いて対象国における移民問題を政治的に争点化し、対象国の政治に影響を与えるものである。

（1）特徴

政治を利用した工作手段は、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、アクターにとって好ましい政治家を支援する上で有利な情報を拡散し、対立候補とって不利な内容の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。

（2）代表的事例

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[24]。

12. インフォメーションを利用した工作手段

コンセプト・モデルでは、「メディア・コントロール及び干渉」「偽情報拡散及びプロパガンダ」「混乱や対立的ナラティブの創出」の 3 つが挙げられている。

・メディア・コントロール及び干渉

対象国メディアを直接支配、または資本関係等を通じて報道内容に介入するものである。

・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、対象国にとって有害な偽情報や悪意ある情報を広範囲に拡散する。

・混乱や対立的ナラティブの創出

対象国内における民族・宗教などに関係した歴史的対立を利用し、社会的分裂を促すナラティブを創出・拡散するものである。

（1）特徴

インフォメーションを利用した工作手段は、人々の思考・判断・価値観に直接作用するため、国家の意思決定や社会の安定に深刻な影響を及ぼす。

近年では、生成 AI による偽動画・偽音声の精度が向上し、印象操作の手段としての有効性が高まっている。その一方で、これらの情報の拡散スピードが加速し、情報量も急増する中でファクトチェックをはじめとする対策が追いついていない状況である。

さらに、民主主義国家では言論・表現の自由が保障されているため、偽情報の拡散に対する脆弱性が顕著である。

また、ハイブリッド戦においては記述の各項でも言及しているとおり、他の工作手段と組み合わせることでより高い効果を発揮するために多用される。

（2）代表的事例

2022 年 3 月、EU はロシアによるウクライナ侵攻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[25]。

13. 技術を利用した工作手段

コンセプト・モデルでは、「技術を利用した工作手段」として「電子戦、特に GNSS（全球測位衛星システム）妨害及びなりすまし」を工作手段として挙げている。

・GNSS 妨害

強力な妨害電波により正規の信号をかき消し、受信機を測位不能にするものである。

・GNSS なりすまし

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。

（1）特徴

GNSS 妨害・なりすましは、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など、社会インフラに深刻な影響を及ぼす。

ハイブリッド戦では、GNSS 攻撃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が行われる可能性がある。また、交通の混乱と偽情報の拡散を組み合わせることで、市民の心理的安全性を阻害することで、政府への信頼を低下させる効果もある。

（2）代表的事例

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[26]。

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[27]。

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。

おわりに

ハイブリッド戦は、軍事・経済・情報・サイバー・文化など多様な領域を横断し、国家や社会の脆弱性を突く複合的脅威である。その手法は年々巧妙化・高度化し、その影響は一般市民にまで及ぶ。こうした現実は、政府による対応を中心とした従来の安全保障の枠組みだけでは十分に対応できないことを浮き彫りにしている。

本稿で整理した 13 のグループ・40 の工作手段は、いずれも現代社会において実際に確認されてきたものであり、今後も新たな手法が登場する可能性が高い。この複合的脅威に対抗するためには、政府や専門機関だけでなく、一般市民を含む社会全体での脅威認識の共有がまず必要である。その上で、各脅威に対する具体的な対策の検討や、国際社会との連携強化、社会における教育・啓発活動の充実など、官民の垣根を超えた多角的なアプローチが求められる。

複雑化するハイブリッド戦への理解を深め、社会全体でレジリエンスを高めていくことが、今後の安全保障において極めて重要となるであろう。

[1] European Commission, & Hybrid CoE, The Landscape of Hybrid Threats: A Conceptual Model Public Version, 2021, p. 33, https://www.hybridcoe.fi/wp content/uploads/2021/02/conceptual_framework reference-version-shortened good_cover_-_publication_office.pdf (2025 年 9 月 1 日閲覧)

[2] 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）。

[3] 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）。

[4] 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）。

[5] 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）。

[6] 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）。

[7] 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）

[8] 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）

[9] 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）

[10] 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）

[11] 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）。

[12] 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）

[13] 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

[14] 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）

[15] «Обращение Президента Российской Федерации» Президент России, 21 сентября 2022,

http://kremlin ru/events/president/news/69390（2025 年 9 月 21 日閲覧）

[16] 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）

[17] 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）

[18] 「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）

[19] 中華人民共和国海警法第 22 条

[20] 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）

[21] 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）

[22] 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）

[23] 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）

[24] 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）

[25] 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）

[26] 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）

[27] “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）

PROFILE

川嶋　隆志

戦史研究センター安全保障政策史研究室所員

専門分野：ハイブリッド戦、WPS (Women, Peace and Security)

防衛研究所企画部企画調整課

直　通：03-3260-3011
代　表：03-3268-3111（内線 29177）
防衛研究所 Web サイト：www.nids.mod.go.jp