

サイバー時代の抑止は何が変わったのか

伝統的理論の限界と新たな抑止の考え方

政策研究部サイバー安全保障研究室 研究員 金子 怜斗

はじめに

「サイバー抑止は死んだ。サイバー抑止よ、永遠なれ！」（“Cyber deterrence is dead. Long live cyber deterrence!”）。この逆説的なフレーズは、チューリッヒ工科大学（ETH Zurich）のマックス・スミーツ（Max Smeets）とステファン・ソエサント（Stefan Soesanto）が 2020 年 2 月に米外交評議会（Council on Foreign Relations）に掲載した論考の見出しである¹。「サイバー抑止は死んだ」という断定調と、「サイバー抑止よ、永遠なれ」という逆説的宣言は、この分野の議論が陥ってきた矛盾を鋭く突いている。サイバー抑止という概念は、誕生以来、約 30 年間の間に理論的隆盛と現実面での行き詰まりを同時に経験してきた。サイバー攻撃が日常化する現代において、「サイバー抑止」という概念はどれほど有効なのか。本稿は、核時代に発展した抑止理論の基本的な枠組みを整理したうえで、米国を中心とするサイバー抑止論の変遷をたどる。また、サイバー時代の抑止において、攻撃をゼロに抑えることは不可能に近い。相手が軍事目的を達成できる可能性を、継続的にそして多層的に削り取っていくことを目指すのが近年の潮流となっている。こうしたなか、近年注目されている累積的抑止、区切りのある抑止やクロス・ドメイン抑止の理論的發展を紹介する。

では、なぜ今この問いを改めて問わなければならないのか。第 1 に、2022 年に始まったロシアによるウクライナ全面侵襲に見られるように、目下、サイバー作戦が他のドメイン（領域）と統合運用されるといふ状況が大規模に実証される現実がある。ウクライナ侵襲当日の衛星通信事業者 ViaSat への攻撃、継続的なワイパー型マルウェアの投入、電力網・通信インフラへの妨害は、サイバー作戦が航空・ミサイル攻撃と連動して実施されたことを示している。もっとも、こうした統合運用が実際にどれほど戦略的効果をもたらしたかについては評価が分かれており²、サイバー作戦の寄与を過大視することには慎重であるべきである。しかし、少なくとも、サイバー手段が独立した強制のツールとしてではなく、他の国家手段と組み合わせて運用されるという形態が実戦において観察されたことは、特筆すべきことである。なお、統合運用の観点から、もっとも直近の事例として、2026 年 2 月に米軍が実施したイランに対するエ

ピック・フューリー作戦（Operation Epic Fury）が挙げられる。米軍制服組トップのダン・ケイン（Dan Caine）統合参謀本部議長は、サイバー軍（USCYBERCOM）と宇宙軍（USSPACECOM）が連携してイランの監視・通信・対応能力を妨害・低下させたうえで、地上、海上、航空戦力が連携して目標を攻撃したと述べた。ケイン統合参謀本部議長は、宇宙・サイバー作戦によって相手の状況把握と統制、効果的な反応能力を麻痺させたうえで、物理攻撃に移ったと説明している³。

第 2 に、中国系脅威グループ「ボルト・タイフーン（Volt Typhoon）」が米国および同盟国の重要インフラに長期間潜伏していたことが明らかにされた事例を通じて、有事に備えて平時からサイバー空間上に足場を築いておく活動の戦略的な意味が注目されるようになったことが挙げられる。こうした活動は直ちに破壊を伴うものではないが、米当局などでは、有事の際に重要インフラへ影響を及ぼすためにかかる活動を用いるよう想定されていたと分析している⁴。そのため、ボルト・タイフーンのような事例は従来の抑止理論が前提としてきたような明確な「攻撃の発生」には当てはまりにくく、適切な理解がなされない場合、「攻撃が起きていない以上、抑止は機能している」と見誤るおそれがある。

では、なぜこうした抑止にかかる理論的考察が必要なのか。19 世紀プロイセンの戦略思想家カール・フォン・クラウゼヴィッツ（Carl von Clausewitz）は主著『戦争論』（*On War*）で、理論の役割を、現象に「安定した光」を当て、諸要素の相互関係を明らかにし、重要なものとそうでないものを見分けやすくすることだと述べている⁵。この認識は、サイバー空間という複雑な現象を考えるうえでも有効である。攻撃の主体、手段、影響の境界が曖昧なサイバー空間では、何を、誰に対して抑止しようとしているのかを見極めるために、理論による整理が欠かせない。

核時代の抑止理論—「出来事中心」の評価の確立

抑止理論は、核の出現と開発によって冷戦時代に発達し、戦略論の変遷を形作ってきた⁶。伝統的な抑止の考え方としては、抑止する側が報復するという脅迫によって攻撃側が行おうとしている行動を思いとどまらせる点にある⁷。核兵器以前の軍事戦略が勝利の追求を中心に置いていたのに対し、バーナード・ブローディ（Bernard Brodie）は 1946 年に「軍の主要目的はこれまで戦争に勝つことであったが、今後は戦争を阻止することでなければならない」と指摘し⁸、来る未来の抑止の戦略の根幹を捉えた。グレン・スナイダー（Glenn Snyder）は 1959 年、米ソの対立構造を念頭に抑止を「拒否的抑止（deterrence by denial）」と「懲罰的抑止（deterrence by punishment）」に類型化した。拒否的抑止とは、相手の攻撃が成功しないと認識させることで行動を思いとどまらせる形態であり、懲罰的抑止とは、攻撃した場合に耐えがたい損害・報復を与えると認識させることで攻撃を思いとどまらせる形態である⁹。この二つは、

明確なエスカレーション段階と可視的なシグナリングを前提として機能していた。さらにトマス・シェリング (Thomas Schelling) がコスト計算とシグナリングの論理を精緻化したことで核抑止論は冷戦期を通じて円熟していった。核抑止が比較的明快であったのは脅威の主体が国家に限定され、攻撃の閾値 (threshold) が核使用や大規模侵攻という明確な行為に集約され、攻撃が起きなければ抑止は成功、起きれば失敗という出来事中心の評価基準もこの構造の中で一定の合理性を持っていた。こうした伝統的抑止理論において、抑止の成立に必要な条件として一般に「3つのC」が重視されてきた。第1は、能力 (Capability) —相手に実際の損害を与えられる軍事的・報復的手段の保有。第2は、信頼性 (Credibility) —「本当に報復するのか」という問いに対して、相手に報復の意思があると信じさせるだけの説得力。第3は、伝達 (Communication) —抑止の意図と能力を相手に伝える手段。この3条件がそろってはじめて、抑止のメッセージは機能すると考えられてきた。

もちろん、抑止理論は通常戦力も含み、合理的なモデルから認知的なモデルまで幅広い議論を取り込んでいる。それでも、抑止の根本的な狙いが「軍事行動の結果を恐れさせ、コストとリスクの計算を通じて相手の行動を踏みとどまらせる」点にある、という構造は変わらない。ジョン・ミアシャイマー (John Mearsheimer) が通常抑止の研究で示したように、核・通常を問わず、侵攻コストが期待利益を大幅に上回ると相手が認識することが抑止の機能する条件である¹⁰。問題は、「相手にコストとリスクを正確に計算させる」ための前提、すなわち「何が起きるか」の明確さが核から離れるほど急速に失われていくという点だ。核の場合、兵器の使用がもたらす壊滅的被害は過去の使用経験とともに広く共有されており、結果の見通しは相対的に鮮明である。これに対し、通常戦力を中心とする状況では結末の不確実性が増し、コストとリスクの評価は格段に複雑になる¹¹。初期の抑止研究は合理性と単純さを重視していたが、その背景には兵器の使用とその影響が比較的明確に想定できるという前提があった¹²。換言すれば、抑止の対象が絶対的破壊をもたらす核から通常戦力へと移るほど、攻撃の結果やコストの明確さが失われて不確実性が増すため、相手にとって割に合わない、という戦略的計算を正確に行わせることは核抑止よりはるかに困難になる。ここで重要なのが、ローレンス・フリードマン (Lawrence Freedman) のいう「狭義の抑止 (narrow deterrence)」である。この概念が指すのは、特定の兵器・特定の戦い方に限定された抑止形態であり、その有効性はまさに結末の明確さによって支えられていた¹³。裏を返せば、適用対象や手段の幅を広げるほど、相手に想定させるコストとリスクの輪郭はぼやけ、抑止の機能は損なわれる。つまり、従来の抑止が「重大な行為が起きるか否か」を基準に成否を評価しやすかったのは、この明確さに支えられた出来事中心モデル (event-centric model) が成り立っていたからである。このモデルは核・通常戦力の領域では比較的良好に機能したが、後述するように、サイバー空間に適用しようとする本質的な矛盾を露呈する。

サイバー空間の抑止の潮流とその適用への構造的障壁

サイバー空間に伝統的な抑止理論を適用しようとする試みは、1990年代から存在した¹⁴。懲罰的抑止や拒否的抑止の論理は、理論上、サイバー空間にも適用可能だと考えられた。前者は、サイバー攻撃すれば耐えがたい損害を伴う重大な報復を受けると相手に認識させることで、後者は、サイバー攻撃しても成功しないと認識させることで、相手の行動を思いとどまらせると論じられた¹⁵。ジョセフ・ナイ (Joseph Nye) は、懲罰と拒否に加え、経済的相互依存関係の深化に着目した「絡み合い (entanglement)」や、違反に対する評判コストを付与する「規範 (norm)」を組み合わせることで、抑止が機能しうると論じた¹⁶。しかし、サイバー空間固有の特性の理解が徐々に進むにつれ、抑止理論の適用を阻む構造的障壁の存在が明らかになってきた。ここでは、一般に指摘される3つの障壁を整理する。

(1) 帰属問題 (Attribution Problem)

抑止の前提条件は、「誰がやったか」を速やかに特定できることである¹⁷。しかしサイバー攻撃では、攻撃者が匿名性を保ちながら第三国のサーバーを踏み台にすることや発信元の偽装が常態化しており、国家による攻撃と犯罪集団による攻撃の区別すら困難な場合が少なくない¹⁸。技術的・法的・外交的なアトリビューションには相当の時間と資源を要し、その間に報復の機会は失われ、抑止の信頼性は著しく損なわれる¹⁹。特に、アトリビューションまでの時間的断絶は、報復の脅威を無効化させるほどの要因となる。これは、3つのCのうち「信頼性 (Credibility)」を根底から脅かす問題である²⁰。

(2) シグナリングの困難性

抑止が機能するためには、能力と意思を相手に「伝達 (communicate)」しなければならない²¹。しかし、サイバー能力保有と展開は基本的に秘匿とされており、自国の能力を公開すればその能力自体が無力化されるジレンマがある²²。核実験やミサイル発射試験のような可視的な能力誇示は、サイバー空間ではきわめて難しく、3つのCのうち伝達 (Communication) が本質的に阻害される²³。さらに攻撃行動と防御行動は見かけ上では類似しているため、相手の意図を読み間違えるリスクが高い²⁴。

(3) 閾値 (Threshold) の曖昧性

核時代の評価枠組みが前提とした明確な閾値は、サイバー空間では存在しない²⁵。データ窃取、偵察、破壊工作、影響工作は明確に切り分けられる別々の行為というより、連続的につながった活動として現れることが多い。そのため、サイバー空間では戦争と平和の境界が本質的に曖昧である²⁶。この構造はスミーツとソエサントが指摘するように、従来の抑止理論が想定してきた「物理レイヤーへの攻撃」とい

う、懲罰的抑止にも拒否的抑止にも共通する脅威発生モデルを中心に組み立てられていた議論の骨格を崩す²⁷。

これらの構造的困難性に加え、サイバー攻撃の非対称性も問題をさらに複雑化させる。防御コストが攻撃コストを上回る現在のサイバー空間では、中小国や非国家アクターでも強大な国家に打撃を与えることができる。この非対称性は、抑止の前提である報復能力の相対的優位性を弱め、国家が保有する伝統的な軍事的優位が必ずしも抑止力に直結しないという現実を生み出している²⁸。また、現在でも多く参照されているトマス・リッド (Thomas Rid) が 2013 年の著書で主張したように、いわゆる「サイバー9.11」や「サイバー・パールハーバー」と呼ばれるような、都市機能を麻痺させ人命に直接影響を与える規模のサイバー攻撃は今のところ現実化していない。リッドの定義によれば、サイバー行為が「戦争」に該当するためには暴力性 (violence)・手段性 (instrumental)・政治的意図 (political) の 3 要件を満たす必要があり、これまでの事例のほとんどはサイバー空間における諜報活動 (espionage)・破壊工作 (sabotage)・社会浸食 (subversion) のカテゴリーに収まるため暴力性がないとされる²⁹。換言すれば、戦争行為ではない以上、そもそも抑止の対象ではなく、核戦争に相当するような出来事も起きていない以上、抑止は「成功」しているとさえ解釈されうる。ロシアが介入したといわれる 2016 年の米大統領選以降、政策的関心が物理的破壊から政治プロセスを標的とした情報戦・影響力工作へと移行したことで、サイバー抑止論への関心は失速した³⁰。しかし問題は、その「成功」の裏側で戦争未満の活動が急速に拡大し、常態化してきたことにある。ここに、出来事中心モデルの限界がある。このモデルでは、戦争未満の浸食を見過ごしやすい。リッドの議論は、サイバー空間でも抑止を論じうる余地を示した一方で、従来の抑止概念だけでは継続的な競争の実態を十分に説明できないことも明らかにした。そこで議論は、攻撃の不発だけを基準にする発想から、平時からの継続的関与を通じて相手の行動を制約する発想へと広がっていく。その延長線上に現れたのが、「サイバー持続性理論 (cyber persistence theory)」である³¹。マイケル・フィッシャーケラー (Michael Fischerkeller)、エミリー・ゴールドマン (Emily Goldman)、リチャード・ハーネット (Richard Harknett) らが提唱する同理論によれば、サイバー空間における国家間の戦略的相互作用の主要形態は「強制 (coercion)」に基づく抑止ではなく「搾取 (exploitation)」である。また、防御側の安全は相手の善意に依存して受動的に確保されるものではなく、継続的な主導権の確保と維持によって形成されると主張する³²。この理論は、2018 年以降に米国防総省がサイバー戦略として採用した「前方防衛 (defend forward)」や、米サイバー軍が作戦レベルで用いる「持続的関与 (persistent engagement)」と通底している³³。2026 年 3 月に発表された米サイバー戦略はこの方針をさらに強化し、「ネットワークへの侵入を許す前に敵対者を検知・対峙・撃破」とするとともに、相手の「能力を侵食し、全国家的手段を用いて攻撃のコストを引き上げる」という、より能動的かつ徹底した姿勢を鮮明にしている³⁴。

サイバー空間と抑止の再考—累積とクロス・ドメインの枠組み

以上のような構造的障壁を踏まえ、サイバー持続性理論は、サイバー空間では強制は成立しないという前提のもとに、抑止理論からの脱却を主張する。しかしサイバー作戦が情報システム等を通じて相手の意思決定に摩擦 (friction) を生み出し、思い通りに動けなくする効果を持つとすれば、その効果を抑止の論理にも応用できるのではないか。実際、米国と英国の公式ドクトリンはその可能性を明示している。米サイバー軍は「サイバー空間の優勢獲得と維持: コマンド・ビジョン (Achieve and Maintain Cyberspace Superiority: Command Vision for USCYBERCOM)」において、継続的関与によって「相手に戦術的摩擦と戦略的コストを課し、防御資源の再配分と攻撃の削減を強いることができる」と明記し、さらに持続的行動を通じて「敵対者の計算に影響を与え攻撃行動を抑止できる」とも述べている³⁵。英国の国家サイバー部隊 (National Cyber Force: NCF) もまた 2023 年のドクトリン文書で、サイバー作戦が「一連の認知的効果 (a range of cognitive effects)」を生み出しうることを、すなわち相手がデータや情報システムに対して持つ信頼を損なうことで意思決定を攪乱しうることを明記している³⁶。

加えて、物理空間との連動という観点からも示唆がある。限界はあるが、ウクライナ戦争においてサイバー作戦が物理空間 (kinetic) の地上作戦と時間的・機能的に連動して運用されたこと、また、最新の事例として 2026 年 2 月のエピック・フューリー作戦を遂行する際、米サイバー軍と宇宙軍が打撃に先立って非物理的 (non-kinetic) な攻勢を実施したとする米軍の公式発表は、サイバー攻勢が物理空間の作戦と結合することで相手の対応能力そのものを剥奪しうることを示している。いずれも現在進行形の事例であり、さらなる研究は必要である。もっとも、サイバー作戦単独では抑止力として完結しないとしても、他の手段と組み合わせることで相手の行動判断に摩擦を与える経路は存在するといえるだろう。こうした認識のもと、以下では代表的な理論展開として、累積的抑止、区切りのある抑止、クロス・ドメイン抑止、そしてこれらの統合的枠組みを順に概観する。

(1) 累積的抑止 (cumulative deterrence)

ユリ・トア (Uri Tor) が提唱した「累積的抑止」は、イスラエルの対テロ・対非正規戦に着目した概念である³⁷。トアは、抑止を「特定の攻撃が起きたか否か」で評価する二分法的モデルから脱却し、当事者同士の断続的な相互作用を通じた学習プロセスとして位置づける。抑止側は繰り返しの応答を積み重ねることで自らのレッドラインを相手に理解させ、サイバー空間におけるゲームのルールを構築・維持しようとする。抑止力は一度確立すれば永続するものではなく、時間とともに減衰するため、特定の脅威や敵対行為に対して繰り返し攻撃を含む反応を積み重ねることで、信頼性を定期的に再充電 (recharging) する必要がある。この勝利の蓄積が長期的に相手の行動変容につながるものであり、限定的な攻撃や反撃

の発生がただちに抑止の「失敗」を意味するわけではなく、それへの対応が次の抑止を構築する材料となりうる³⁸。

この理論の核心はトアが「価格表 (price tag)」と呼ぶ仕組みにある。特定の敵対行為に対して相手が支払うべき代償のメニューを設定し、繰り返し執行することで相手の行動を制限・形成 (restricting and shaping) する。執行手段はサイバー空間内の報復にとどまらず、攻勢的カウンター・サイバー攻撃、物理的軍事手段 (kinetic military tools)、外交・金融ツールを包含するクロス・ドメインの措置が想定されており、攻撃をゼロにすることではなく反復的な応答を通じた相手の行動パターンの変容が目標とされる³⁹。サイバー空間のように部分的な攻撃が常態化している環境においては、この累積的視点は特に示唆に富む。

(2) 区切りのある抑止 (punctuated deterrence)

区切りのある抑止は、累積的抑止と問題意識を共有している。小規模な敵対行為が少しずつ積み重なることに注目するという出発点は共通しており、抑止を静的な「あるかないか」の問いではなく動的なプロセスとして捉える点でも同様である。ただしその対処の論理は異なる。

ルーカス・ケロー (Lucas Kello) は、平時でも武力紛争でもない非平和 (unpeace) という曖昧な競争状態を概念化し⁴⁰、これへの応答として「区切りのある抑止」を提唱した。ケローが注目したのは、サイバー攻撃が単発ではなく、一定期間にわたるキャンペーンとして累積的に遂行されるという構造である。そのため抑止側も個別インシデントに都度反応するのではなく、一連の敵対行為とその累積的効果 (cumulative effects) を一括して対抗措置を講じる対象とするべきだとする⁴¹。ただし懲罰対象の選別は慎重でなければならない。低レベルの犯罪行為と選挙介入などの戦略的行為を無差別に束ねると、相手にどのラインが本当に許容できないのかという混合シグナルを与えてしまう。国家安全保障上の利益全体にわたる集約された効果 (aggregating effects) を推定した上で戦略的レベルの活動のみを厳選して束ねることで、明確なレッドラインを構築すべきだとする⁴²。

実際の対応としては、小さな浸食が積み重なった段階で「一括化 (bundling)」した報復を集中的に加える「単発の噴出 (single burst)」という方式をとる⁴³。相手が仕掛けてくる戦いに受動的に應じるのではなく、過去に累積した敵対行為に対して被害側が定義した時間・場所・手段で報復する。これをケローは「後方への罰 (punishing backward)」と呼ぶ⁴⁴。高度なサイバー能力は一度使うとパッチで無効化されやすいため、報復を一括化することで資源と行政能力を節約することができる⁴⁵。この報復の核心的な目的は物理破壊そのものよりも、耐えがたいコストを与えることで相手の戦略的メリットの計算を修正し、その心理的基盤を変容させることにある⁴⁶。攻撃者が「この程度の攻撃ならコストを払わずに済む」と考えている安易な見積もりに対し、一括した大きな代償を与えることでその期待をリセットさせる。この

際、報復は必ず可視的でなければならない⁴⁷。隠密な報復では攻撃者当人にしかメッセージが届かず、他の潜在的な攻撃者への警告にならないからだ。抑止の本質は将来の行動を制限するための一連のコミュニケーション、いわゆるシグナリングであり、公然の反撃こそが相手の心理的・戦略的計算を長期にわたって変容させる力となる。さらに手段はサイバー領域に限定されず、「争点連結 (issue linkage)」の論理から経済制裁・外交措置・軍事的シグナリングなど自国が優位にある領域を組み合わせることで、サイバー単独では確保しにくい抑止の信頼性と心理的重みを補完する⁴⁸。この意味で、区切りのある抑止はクロス・ドメイン抑止の理論的前提と通底している。

(3) クロス・ドメイン抑止

クロス・ドメイン抑止とは、ある領域（ドメイン）における敵対行為を思いとどまらせるために、異なるドメイン、あるいは複数のドメインを組み合わせた脅威を用いる戦略である⁴⁹。サイバー空間においては、アトリビューションの困難さやサイバー武器の秘匿性・限定的な再利用性といった特性から、同一ドメイン内のみでの抑止（サイバー対サイバー）には限界があるという考えのもと、このアプローチが不可欠な代替案として議論されている⁵⁰。その理論的基礎は、サイバー・パワーは単独で決定的となることは稀であり、外交、情報、軍事、経済（DIME）といった国家権力の諸手段を統合し、陸・海・空・宇宙・サイバーという5つの運用環境を横断して相手の特定の活動を阻止することである⁵¹。

このクロス・ドメインの視点を包括的な防衛構想へと昇華させたのが、米国の「統合抑止 (Integrated Deterrence)」である⁵²。米国防大学 (National Defense University: NDU) の議論では、DIME、民間セクター、同盟国といった「多側面」の要素と、情報収集 (レベル0) から核 (レベル5) に至るエスカレーション段階を組み合わせた「多層的アーキテクチャ」が提示されている⁵³。この枠組みにおいてサイバー作戦とサイバーによる影響工作作戦は、武力紛争閾値未満の「レベル2」だけでなく、閾値以上の物理的破壊を伴う「攻勢的サイバー・物理複合作戦」である「レベル3」として、通常戦力 (レベル4) や核 (レベル5) とシームレスに統合され、全ドメインにまたがる戦略的圧力の総体として運用される⁵⁴。このような統合的なアプローチにより、特定の戦略的文脈に応じた比例的かつ実効的な応答を可能にすることで、攻撃者にコストが便益を上回ると認識させることが目指されることは、2023年の米国防総省のサイバー戦略にも記されている通りである⁵⁵。

(4) 抑止の横断的統合

以上3つのアプローチを横断的に統合しようとする最新の試みとして注目されるのが、英国王立国防安全保障研究所 (RUSI) のルイーズ・マリー・ヒュレル (Louise Marie Hurel) とギャレス・モット (Gareth Mott) が2025年8月に発表したレポート「多極化世界でサイバー抑止を再考する (Rethinking Cyber Deterrence in a Multipolar World)」である⁵⁶。同レポートは、これまでのサイバー抑止論を5つの立場と

して整理する。これは、①核抑止アナロジー（相互確証破壊の論理をサイバーに援用）、②懐疑論（サイバーへの抑止理論の適用そのものに疑義）、③持続的関与（サイバー空間での常時接触による摩擦の蓄積）、④レジリエンス優先（攻撃の防止より被害吸収力の構築）、⑤クロス・ドメイン抑止（複数領域の手段の統合）からなる。いずれも有益な示唆を持つが、単独ではロシア・中国・イランなど複数の国家が競合する多極的・グレーゾーンの現在の脅威環境に対応しきれないと同レポートは指摘する。例えば、核アナロジーはサイバー能力の限定性と一過性を看過し、懐疑論は政策的な行動を麻痺させる。持続的関与はエスカレーション管理の問題を内包し、レジリエンスのみでは攻撃者に政治的・戦略的な代償を課せない。クロス・ドメイン抑止は方向性として有望だが、政府横断的な調整とエスカレーション管理の困難という現実的課題を抱えている⁵⁷。

こうした各立場の限界を踏まえ、ヒュレルとモットは「累積的、クロス・ドメイン統合アプローチ」を提唱する。平時の監視・外交的警告といった低強度の予防的関与から、制裁・サイバー作戦・軍事的シグナリングといった高強度の対応まで、連続する手段の組み合わせとして設計すべきだという考え方である。このアプローチには、5つの特性がある。すなわち、クロス・ドメイン（外交・経済・軍事を含む政府全手段の動員）、累積的（一回限りの作戦ではなくキャンペーンによる持続的効果の蓄積）、反復的・学習的（試行錯誤を通じて戦略を適応させる学習プロセス）、最適化（tailored）（相手の戦略文化や文脈を考慮した相手国特定型の抑止設計）、グレーゾーン志向（武力紛争と平時の間のグレーゾーンにおける優位の最大化）の5つである。このアプローチは、閾値未満の悪意ある活動を抑制しつつ、深刻な侵害に対してはより力強い対応の地ならしをするという段階的な抑止の実効性を追求するものであり⁵⁸、累積的抑止・区切りのある抑止・クロス・ドメイン抑止という本節で概観した3つのアプローチを統合する実践的枠組みとして、今後の政策形成に示唆を与えるものとなっている。

おわりに

核時代に確立された抑止理論は、「重大な攻撃が起きなければ成功」という出来事中心の評価基準を持ち、明確な閾値・可視的な脅威主体・二分法的な平和と戦争を前提としていた。サイバー空間はこれらの前提を根底から覆す。帰属の困難、グレーゾーンの常態化、情報システムへの攻撃、非国家アクターの多様性といった要素は従来の計算に基づく抑止モデルが想定していなかった変数である。

スミーツとソエサントが2020年に「サイバー抑止は死んだ」と宣言したのは、この構造的限界への率直な認識である。しかし彼らが同時に「長生きせよ」と続けたのは、概念が失効したのではなく、従来

の適用形態が失効したに過ぎないという認識による。サイバー抑止論は今後、伝統的な抑止の精緻化と、サイバー空間固有の論理に即した新概念の開発という二つの方向で展開すると予測される。

クラウゼヴィッツが示したように、理論の使命は唯一解を提供することではなく、現象に安定した光を当て、重要なものとそうでないものを分離し、思考の自由な展開を可能にすることである。サイバー抑止に関する理論的考察もまた、「これが正解だ」という解答を求めるものではなく、複雑な現実を見通すための概念的枠組みを鍛え続けることにその価値がある。

¹ “Cyber Deterrence Is Dead. Long Live Cyber Deterrence!,” Council on Foreign Relations, February 18, 2020, <https://www.cfr.org/articles/cyber-deterrence-dead-long-live-cyber-deterrence>.

² Jon Bateman, *How Militarily Effective Have Russia's Cyber Operations Been in Ukraine?*, *Russia's Wartime Cyber Operations in Ukraine*: (Carnegie Endowment for International Peace, 2022), pp. 5–31, <https://www.jstor.org/stable/resrep45856.5>; Jon Bateman, *Why Have Russian Cyber Operations Not Had Greater Strategic Impact?*, *Russia's Wartime Cyber Operations in Ukraine*: (Carnegie Endowment for International Peace, 2022), pp. 32–44, <https://www.jstor.org/stable/resrep45856.6>.

³ “Secretary of War Pete Hegseth and Chairman of the Joint Chiefs of Staff Gen. Dan Caine Hold a Press Briefing,” U.S. Department of War, March 2026, <https://www.war.gov/News/Transcripts/Transcript/Article/4418959/secretary-of-war-pete-hegseth-and-chairman-of-the-joint-chiefs-of-staff-gen-dan/>.

⁴ United States Department of Justice, “U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure,” January 31, 2024, <https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>.

⁵ Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton University Press, 1989), p. 578.

⁶ Lawrence Freedman and Jeffrey H. Michaels, *The Evolution of Nuclear Strategy: New, Updated and Completely Revised*, Fourth edition (Palgrave Macmillan, 2019), p. 5.

⁷ Patrick M. Morgan, *Deterrence: A Conceptual Analysis*, Second edition, (Sage Publications, 1983), p. 26; Lawrence Freedman, *Deterrence* (Polity Press, 2004), p. 6.

⁸ Bernard Brodie, “Implications for Military Policy,” in *The Absolute Weapon: Atomic Power and World Order*, ed. Bernard Brodie (New York: Harcourt, Brace and Company, 1946), p. 62.

⁹ Glenn Snyder, *Deterrence by Denial and Punishment*, Woodrow Wilson School of Public and International Affairs. Center of International Studies. Research Monograph, No. 1 (Woodrow Wilson school of Public and International Affairs, Center of International Studies, Princeton University, 1959), <https://catalog.hathitrust.org/Record/005407396>.

¹⁰ John J. Mearsheimer, *Conventional Deterrence* (Cornell University Press, 1983), p. 23, <https://www.jstor.org/stable/10.7591/j.ctt1rv61v2>.

¹¹ *ibid*, p. 35.

¹² *ibid*, p. 27.

¹³ Freedman, *Deterrence*, p. 21.

- ¹⁴ James Der Derian, "Cyber-Deterrence," WIRED, September 1, 1994, <https://www.wired.com/1994/09/cyber-deter/>.
- ¹⁵ Dorothy Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Forces Quarterly*, (April 2015), <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/581864/rethinking-the-cyber-domain-and-deterrence/>; Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies*, vol. 46, no. 3 (2023): pp. 534–569, <https://doi.org/10.1080/01402390.2021.1944856>.
- ¹⁶ Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security*, vol. 41, no. 3 (2017): pp. 44–71, https://doi.org/10.1162/ISEC_a_00266.
- ¹⁷ Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option*, 1st ed (Rowman & Littlefield Publishers, Incorporated, 2017), pp. 71–72; Aaron Franklin Brantly, ed., *The Cyber Deterrence Problem* (Rowman & Littlefield International, 2020), p. 7.
- ¹⁸ Timothy M. McKenzie, *Challenges for Cyber Deterrence, Is Cyber Deterrence Possible?* (Air University Press, 2017), p. 8, <https://www.jstor.org/stable/resrep13817.9>; Jasper, *Strategic Cyber Deterrence*, p. 48, 89.
- ¹⁹ Jacquelyn G. Schneider, "Deterrence in and through Cyberspace," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Eric Gartzke and Jon R. Lindsay (Oxford University Press, 2019), p. 116, <https://doi.org/10.1093/oso/9780190908645.003.0005>; Louise Marie Hurel and Gareth Mott, "Rethinking Cyber Deterrence in a Multipolar World," The Royal United Services Institute for Defence and Security Studies, August 20, 2025, p. 6, <https://www.rusi.org/explore-our-research/publications/emerging-insights/rethinking-cyber-deterrence-multipolar-world>; Michael P. Fischerkeller et al., "The Limits of Deterrence and the Need for Persistence," in *The Cyber Deterrence Problem*, ed. Aaron F. Brantly (Bloomsbury Publishing USA, 2020), p. 27.
- ²⁰ Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies*, vol.40, no. 1–2 (2017): 100, <https://doi.org/10.1080/01402390.2015.1115975>; Peter Pijpers and Kraesten Arnold, "Rethinking Cyber Deterrence: Adapting to the Realities of the Digital Battlefield," *Journal of Strategic Security*, vol. 18, no. 1 (2025): p. 66; Jasper, *Strategic Cyber Deterrence*, p. 60.
- ²¹ Thomas C. Schelling, *The Strategy of Conflict* (Harvard Univ. Pr, 1960), pp. 13–18.
- ²² Borghard and Lonergan, "Deterrence by Denial in Cyberspace," p. 557; Erica D. Lonergan, "Minding the Gap? The Strategic Logic of Cyber Coercion in Theory and Practice," *Journal of Strategic Studies* (2025): p.7, <https://doi.org/10.1080/01402390.2025.2565191>; Pijpers and Arnold, "Rethinking Cyber Deterrence," p. 64.
- ²³ Schneider, "Deterrence in and through Cyberspace," p. 116; Hurel and Mott, "Rethinking Cyber Deterrence in a Multipolar World," p. 6; Fischerkeller et al., "The Limits of Deterrence and the Need for Persistence," p. 27.
- ²⁴ Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, vol.26, no. 3 (2017): p. 456, <https://doi.org/10.1080/09636412.2017.1306396>; Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity* vol. 1, no. 1 (2015): p. 55, <https://doi.org/10.1093/cybsec/tyv003>.
- ²⁵ Lucas Kello, *Striking Back, The End of Peace in Cyberspace - And How to Restore It* (Yale University Press, 2022), p. 142, <https://doi.org/10.2307/j.ctv2v55b54.10>.
- ²⁶ Nye, "Deterrence and Dissuasion in Cyberspace," p. 48; Fischerkeller et al., "The Limits of Deterrence and the Need for Persistence," p. 26.
- ²⁷ Max Smeets and Stefan Soesanto, "Cyber Deterrence Is Dead. Long Live Cyber Deterrence!," February 18, 2020, <https://www.cfr.org/articles/cyber-deterrence-dead-long-live-cyber-deterrence/>; Michael P. Fischerkeller et al., *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford University Press, 2022); Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis*, vol. 61, no. 3 (2017): p. 381, <https://doi.org/10.1016/j.orbis.2017.05.003>.
- ²⁸ Ben Buchanan, "Limitations, Objections, and the Future of the Cybersecurity Dilemma," in *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, ed. Ben Buchanan (Oxford University Press, 2017), p. 154, <https://doi.org/10.1093/acprof:oso/9780190665012.003.0008>.

-
- ²⁹ Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013), pp. 14–18, 19–29.
- ³⁰ Smeets and Soesanto, "Cyber Deterrence Is Dead. Long Live Cyber Deterrence!"
- ³¹ Richard Harknett and Emily Goldman, "The Search for Cyber Fundamentals," *Journal of Information Warfare*, vol.15, no. 2 (2016): pp. 81–88; Fischerkeller et al., *Cyber Persistence Theory*.
- ³² Fischerkeller et al., *Cyber Persistence Theory*, p. 1.
- ³³ USCYBERCOM, "Achieve and Maintain Cyberspace Superiority Command Vision for US Cyber Command," 2018, <https://www.cybercom.mil/portals/56/documents/uscybercom%20vision%20april%202018.pdf>; U.S. Department of Defense, "Summary: Department of Defense Cyber Strategy 2018," 2018, <https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategy2018.pdf>.
- ³⁴ The White House, "President Trump's Cyber Strategy for America," March 2026, <https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf>.
- ³⁵ *ibid.*
- ³⁶ UK National Cyber Force, "Responsible Cyber Power in Practice," GOV.UK, April 4, 2023, <https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html>.
- ³⁷ Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence."
- ³⁸ *ibid.*, pp. 94–95, 102, 105.
- ³⁹ *ibid.*, p. 108.
- ⁴⁰ Lucas Kello, *Striking Back, The End of Peace in Cyberspace - And How to Restore It* (Yale University Press, 2022), p. 11, <https://doi.org/10.2307/j.ctv2v55b54.3>.
- ⁴¹ *ibid.*, pp. 141–150.
- ⁴² *ibid.*, p. 152.
- ⁴³ *ibid.*, p. 144.
- ⁴⁴ *ibid.*, p. 148.
- ⁴⁵ *ibid.*, p. 144.
- ⁴⁶ *ibid.*, pp. 143–44, 157.
- ⁴⁷ *ibid.*, p. 157.
- ⁴⁸ *ibid.*, pp. 154–157.
- ⁴⁹ Jon R. Lindsay and Erik Gartzke, "Introduction: Cross-Domain Deterrence, from Practice to Theory," in *Cross-Domain Deterrence: Strategy in an*

Era of Complexity, ed. Eric Gartzke and Jon R. Lindsay (Oxford University Press, 2019), p. 4, <https://doi.org/10.1093/oso/9780190908645.003.0001>.

⁵⁰ Schneider, "Deterrence in and through Cyberspace," p. 96, 104.

⁵¹ Michael Navicky and Benjamin Tkach, "Cross-Domain Cyber Incidents and State Responses," in *Integrated Deterrence and Cyberspace: Selected Essays Exploring the Role of Cyber Operations in the Pursuit of National Interest*, ed. Joseph L. Billingsley, Strategic Monographs (National Defense University Press, 2023), p. 24, <https://digitalcommons.ndu.edu/strategic-monographs/3/>.

⁵² Heidi Berg, "Introduction," in *Integrated Deterrence and Cyberspace: Selected Essays Exploring the Role of Cyber Operations in the Pursuit of National Interest*, Strategic Monographs (National Defense University Press, 2023), p. xiii, <https://digitalcommons.ndu.edu/strategic-monographs/3/>.

⁵³ Jim Chen, "Deterrence in Cyberspace: An Essential Component in Integrated Deterrence," in *Integrated Deterrence and Cyberspace Selected Essays Exploring the Role of Cyber Operations in the Pursuit of National Interest*, Strategic Monographs (National Defense University Press, 2023), p. 10.

⁵⁴ *ibid*, p. 10.

⁵⁵ U.S. Department of Defense, "Summary 2023 Cyber Strategy of the Department of Defense," September 2023, <https://www.war.gov/News/Releases/Release/Article/3523199/dod-releases-2023-cyber-strategy-summary/>.

⁵⁶ Hurel and Mott, "Rethinking Cyber Deterrence in a Multipolar World."

⁵⁷ *ibid*, pp. 5-9.

⁵⁸ *ibid*, p. 10.

PROFILE

金子 怜斗

政策研究部サイバー安全保障研究室 研究員

専門分野：戦争学、サイバー・認知領域の安全保障、抑止論、ミサイル戦略

本欄における見解は、防衛研究所を代表するものではありません。
NIDS コメンタリーに関する御意見、御質問等は下記へお寄せ下さい。
ただし記事の無断転載・複製はお断りします。

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