KCS Report

No. 01

ウクライナから東アジアへ

―新領域における戦いとその教訓―

土屋大洋、川口貴久、佐々木孝博、八塚正晃、山本達也

戦　略　構　想　セ　ン　タ　ー

KEIO CENTER FOR STRATEGY

本報告書は、東京海上ディーアール株式会社が企画・運営する「台湾有事におけるサイバー戦・情報戦」研究プロジェクト（研究代表：土屋大洋）の成果の一部である。プロジェクトでは、平野高志氏（ウクライナ『ウクルインフォルム通信』編集者）、李世暉氏（台湾・国立政治大学教授）、鄭子眞氏（台湾・中国文化大学教授）、沈伯洋氏（台湾・台北大学大学院犯罪学研究科助理教授）、早川友久氏（日本台湾交流協会台北事務所広報文化室長）、須藤龍也氏（朝日新聞編集委員）から貴重な知見を得た（順不同）。感謝申し上げる。

2024 年 2 月 6 日

編集・発行　　慶應義塾大学グローバルリサーチインスティテュート（KGRI）戦略構想センター

問い合わせ先　　〒108-8345　東京都港区三田 2-15-45

KEIO CENTER FOR STRATEGY

要旨

2022 年 2 月 24 日、ロシア軍はウクライナ領土に全面侵攻し、今日までウクライナ軍とロシア軍による攻防が続く（便宜上、これを「ウクライナ戦争」と呼ぶ）。開戦直後から、想定外のロシアの苦戦とウクライナの善戦は各国の政策当局者、インテリジェンス関係者、研究者等にとって大きな関心事であり続けている。それゆえ、ウクライナ戦争の終結が見えない中でも、この戦争から「教訓」を導き出そうとする試みは少なくない。こうした試みの対象は、陸、海、空といった伝統的戦闘領域のみならず、宇宙、サイバー、電磁波、認知領域といった新しい戦闘領域も含まれる。

同様に、本報告書も現時点での「教訓」抽出を試みる。具体的には、ウクライナ戦争からの教訓や示唆は将来の紛争にどこまで適用可能なのか、特に台湾有事といった中国が関与する紛争でどこまで再現可能なのか、という点を検討する。本報告書は特に①宇宙・サイバー・電磁波・認知といった新領域そのもの、②新領域と伝統的領域（陸・海・空）の相互作用に注目し、この問いに答える。

もちろん、ウクライナ戦争の特殊性を鑑みれば、この戦争で生じた事実を一般化することは困難や限界が伴う。また、ウクライナ戦争の教訓の全てや台湾有事への備えとして必要な事項を網羅するものではない。本報告書は、作戦領域の拡大、ロシア流の戦争、中国による学習、テック企業の関与、政治体制等の観点から、以下を「ウクライナ戦争からの教訓」「台湾有事への備え」として提言する。

- 全般： 先端技術の防衛分野への適用・実装の迅速化
- 全般： テック企業との協力と連携
- 宇宙領域： 多軌道衛星通信を含む有事の通信レジリエンスの向上
- サイバー・認知領域： 一元化された状況認識・対処体制の確立
- サイバー領域： 「積極的サイバー防御」体制の早期実現
- 認知領域： プラットフォーム上の状況認識能力の強化（認知戦の「守り」）
- 認知領域： 戦略的コミュニケーションの強化（認知戦の「攻め」）
- 電磁波領域： 有事を想定した電磁波管理
- 伝統的領域との融合： 無人機作戦への備え

目次

はじめに

土屋 大洋、川口 貴久

2022 年 2 月 24 日、ロシア軍はウクライナ領土に全面侵攻した。開戦前後、多くの専門家の見立てでは、ウクライナの首都キーウは数日以内に陥落し、ボロディミル・ゼレンスキー（Volodymyr Zelenskyy）政権は崩壊し、そしてウクライナはロシアの支配・影響下におかれるはずだった。しかし、この予測は外れた[1]。その後、ロシアによるウクライナ全面侵攻（便宜上、「ウクライナ戦争」と呼ぶ）の主戦場は、ドンバス地方と南部に移行する。詳細は割愛するが、本報告書の脱稿時点（2023 年 12 月）でも、ウクライナ軍とロシア軍による攻防が続く。

開戦直後から、想定外のロシアの苦戦とウクライナの善戦は各国の政策当局者、インテリジェンス関係者、研究者等にとって大きな関心事であり続けている。それゆえ、ウクライナ戦争の終結が見えない中でも、この戦争から「教訓」を導き出そうとする試みは少なくない[2]。

こうした試みの対象は、陸、海、空といった伝統的戦闘領域のみならず、宇宙、サイバー、電磁波、認知領域といった新しい戦闘領域も含まれるが、両者では文脈がやや異なる。現時点でウクライナ戦争は地上兵力と火力が勝敗を決する「20 世紀」型の戦争の様相を呈しているからだ。つまり、ウクライナ戦争が 2014 年のクリミア併合とドンバス紛争ほど「ハイブリッド」ではなかったこと、ロシアのサイバー戦、電子戦、情報戦が事前の予想ほど成果をあげていないことに焦点が当たる。

ウクライナ戦争からの教訓と示唆

こうした分析の多くと同様に、本報告書の関心は次の点に集約される。つまり、ウクライナ戦争からの教訓や示唆は将来の紛争にどこまで適用可能なのか、特に台湾有事といった中国が関与する紛争でどこまで再現可能なのか、というものだ。本報告書は特に①宇宙・サイバー・電磁波・認知といった新領域そのもの、②新領域と伝統的領域（陸・海・空）の相互作用に注目して、この問いに答える。

もちろん、ウクライナ戦争の特殊性を鑑みれば、この戦争で生じた事実を一般化することは困難や限界が伴う。ロシアによる軍事行動は国連憲章を含む既存の国際法に明らかに違反した侵略行為であることに疑いの余地はない。ロシア流の戦争、特にサイバー戦・情報戦にはロシア固有の要素があるし、ウラジーミル・プーチン（Vladimir Putin）大統領の戦略的計算と意思決定は外部からみると評価が困難だ。2014 年のクリミア併合以降、ウクライナがハイブリッド戦争への対処も含めて、安全保障・防衛分野に投資を継続してきた事実も見過ごせない。

本報告書はこうした特殊性や固有事情を踏まえつつ、将来の戦争で適用可能な教訓や示唆を模索する。

台湾有事

さらに本報告書は「教訓」「示唆」の具体的な適用先として台湾有事を想定し、適用可能性と限界を検討する。中国人民解放軍の急速な軍備強化を背景に、特にウクライナ戦争やナンシー・ペロシ（Nancy Pelosi）米下院議長の訪台に伴う軍事的緊張（2022 年 8 月）以降、台湾有事への懸念が急速に高まっている。それゆえ、既に「北京はウクライナ戦争から何を学んでいるのか」という観点で議論が行われてきた。ロシアと中国、ウクライナと台湾の相違をふまえて、過度な一般化を排した「誤った教訓（wrong lessons）」を論じるものもある[3]。

そもそも、「台湾有事」といっても想定される事態や深刻度は多様だ。異なる複数の有事の端緒、過程、結果が存在する。しかし、多くの専門家の分析や評価を踏まえると、台湾有事のシナリオは①大陸から台湾島に数十万単位の中国人民解放軍が着上陸する「全面侵攻」シナリオ、②台湾が実効支配する東沙諸島、南沙諸島の太平島、福建省沿岸の金門島・馬祖列島等の「島嶼制圧」シナリオ、③直接的に武力を行使しない「『グレーゾーン』での統一」シナリオに整理できる[4]。

「グレーゾーン」とは純然たる有事（黒）でも平時（白）でもない領域を指す。ただし、グレーゾーンにも「濃淡」がある。「白」に近いグレーとして、偽情報・ディスインフォメーション流布、台湾内の親大陸派への支援、対中依存度の高い物資・経済関係の縮小（いわゆる、「経済的威圧」や経済的依存関係の「武器化」）があげられ、これは日常的に確認されている。他方、重要インフラの機能を停止させる破壊的サイバー攻撃、台湾の要人暗殺・ゲリラ活動、海上封鎖（その名称が「検疫」「税務調査」等、何であれ）は「黒」に近いグレー、すなわち本格有事に近い事態といえる。

いずれにせよ、本報告書は台湾有事の中でも、本格的軍事行動や「黒」に近いグレーゾーンといった烈度の高い有事、すなわち「台湾有事は日本有事」という言葉が当てはまる状況を想定する。

本報告書の構成

このように、本報告書は新領域に注目して、ウクライナ戦争から台湾有事に適用できる教訓や示唆を分析する。構成は次の通りである。

第１章（土屋大洋）は、歴史的な作戦領域の拡大、すなわち、陸、海、空、宇宙、サイバースペース、そして認知領域への拡大のプロセスにおける技術の役割について論じる。

第２章（佐々木孝博）は、ロシアが志向する「全領域での戦い」、つまり宇宙、サイバー、情報、電磁波領域の戦い、AI を駆使した戦い、伝統的な物理的な領域での戦いを考察する。ウクライナ戦争で露呈した、こうした「ロシア流の戦争」の欠点や課題をふまえ、台湾有事の観点から教訓や中露の安全保障協力の可能性を論じる。

第３章（八塚正晃）は、中国国内で発表されている論考を手掛かりにして、中国がウクライナ戦争をどのように評価し、いかなる教訓を引き出しているかを析出することを試みる。とりわけ、サイバー、宇宙、認知などの新領域の戦いに対する評価に注目しつつ、今後の中国人民解放軍の軍隊建設との方向性にいかなる示唆を与えうるかを検討する。

第４章（川口貴久）は、ウクライナ戦争におけるサイバー領域の戦いについて、米欧のテック企業による前例のない支援に焦点を当てる。開戦前からのウクライナの準備に加えて、アマゾン、グーグル、スペース X、マイクロソフトといったテック企業の支援はロシアのサイバー戦と戦う上で重要であった。しかし、この成功と教訓は将来の東アジアの紛争、特に台湾有事で再現できるかは極めて疑わしい。

第５章（山本達也）は、政治体制とサイバーセキュリティに関する現状と課題についての論点を提示する。とりわけ、「インターネットの自由」をめぐる国際的な環境変化についてデータも使いながら近年の推移を分析し、サイバーセキュリティと民主主義との関係性について検討する。

第６章（著者一同）では、これまでの議論をふまえて、教訓と提言をまとめる。

[1] ロシア軍による短期決戦が失敗した要因として、キーウ近郊のアントノウ国際空港の防衛、ゼレンスキー大統領自身が亡命を拒否したことが指摘される。小泉悠『ウクライナ戦争』ちくま新書、2022 年、100-115 頁。

[2] 例えば戦争初期のものに Joseph S. Nye, Jr., "Eight Lessons from the Ukraine War," Project Syndicate, June 15, 2022.

[3] Thomas Corbett, Ma Xiu, and Peter W. Singer, "What Is China Learning from the Ukraine War? From battlefield concepts to geopolitics, Beijing is sure to be watching with avid interest—and some chagrin," *Defense One*, April 1, 2022; David Sacks, "What Is China Learning From Russia's War in Ukraine? America and Taiwan Need to Grasp—and Influence—Chinese Views of the Conflict," *Foreign Affairs*, May 16, 2022; Franz-Stefan Gady, "6 Wrong Lessons for Taiwan from the War in Ukraine: A potential Asian war would look very different," *Foreign Policy*, November 2, 2022.

[4] この分類に最も近いものは、神保謙「台湾有事と日米同盟」『交流』No.965、2021 年 8 月、1-4 頁。この他、台湾有事のシナリオを体系的に整理したものとして、Ian Easton, "China's Top Five War Plans," Project 2049 Institute, January 2019; Robert D. Blackwill & Philip Zelikow, *The United States, China, and Taiwan: A Strategy to Prevent War*, New York: Council on Foreign Relations, Feb 2021; 佐藤武嗣、土居貴輝、園田耕司、冨名腰隆「(台湾海峡　にらみ合う大国：１）米中危機、４つのシナリオ」『朝日新聞』2021 年 6 月 6 日; 村野将「台湾防衛戦略：米国の出方を読む」『正論』2021 年 9 月号、48-55 頁; 門間理良「台湾海峡有事における課題と方策」、武田康裕編著『在外邦人の保護・救出：朝鮮半島と台湾海峡有事への対応』東信堂、2021 年、227-252 頁。

第１章
作戦領域の拡大と技術の役割

土屋 大洋

はじめに

第二次世界大戦時の英国首相だったウィンストン・チャーチル（Winston Churchill）は、「思いどおりに進む戦争などあるはずがない。なじみのない海原に船を出し、潮の流れや嵐の激しさが正しく読めることなどあるはずがない。戦争熱に浮かされた政治家は、開戦の号砲が鳴った瞬間、それまで政策の決め手であった自分が、予測もできない、自分の力ではどうにもならない事態の推移にただ翻弄される身となることを悟らなければならない[1]」と言ったという。この言葉は 21 世紀に入って始まったウクライナとガザにおける二つの戦争にもまさに当てはまる。短期で終わると見込まれていたロシアによるウクライナ侵攻は 1 年をゆうに超え、まもなく 2 年になろうとしている。ハマスによるミサイル攻撃によって突如として始まったガザにおける戦争も、2023 年末現在、長期化の様相を見せはじめている。

21 世紀に入って新たな戦争が起こるとは多くの人が予測していなかった。しかし、21 世紀に入って 20 年も経ってから始まった戦争は、やはり従来のものとは異なる側面も見せている。それは、作戦領域の拡大と複合化である。

歴史的に見れば、陸、海、空、宇宙、サイバースペース、そして認知領域へと、作戦領域は徐々に拡大しつつあるが、そのプロセスにおいて技術がどのような役割を果たしてきたのかを本報告書全体の前置きとして本章では見ておきたい。

1. 作戦領域の拡大

技術が安全保障に大きな役割を果たすことは直感的に理解しやすい。例えば、核兵器の登場は 20 世紀後半以降の戦争の在り方を大きく変えることになった。その 1 つの帰結は冷戦

であろう。イデオロギー的に対峙する勢力が、それぞれ相手を何度も殲滅させられるだけの兵力を持ちながら、それを使うことを躊躇するというまれに見る時代が数 10 年続き、それが時に「長い平和」とさえ呼ばれた[2]。

音楽における三和音をトライアド（triad）と呼ぶが、核のトライアドというときには、爆撃機、ミサイル、潜水艦の 3 つを指す。核兵器を敵目標に運ぶ手段としてそれらが使われるからである。しかし、そうした核のトライアドは、最初に宇宙の軍事化によって影響を受けることになった。第二次世界大戦中に発明されたナチス・ドイツの V2 ロケットが弾道ミサイルの元祖だとすれば、それが発明されたときには人工衛星は使われていなかった。世界最初の人工衛星スプートニクが打ち上げられたのは 1957 年である。その後、宇宙空間はソ連と米国がしのぎを削り、偵察衛星レジームとも呼ばれたスパイ衛星による監視の時代へ入った。使えない核をいっそう使えないものにするためにスパイ衛星による相互監視は必要悪として受け入れられた。

しかし、宇宙はスパイ衛星によってはるか上空から眺めるためだけの空間ではなかった。全地球測位システム（GPS）が実用化されると、地球上の任意の一点を正確に認識できるようになり、精密誘導兵器が使えるようになった。他方、ミサイル誘導だけでなく、戦闘機や艦船などあらゆる兵器システムが GPS に依存すればするほど、逆に宇宙システムの傍受や破壊も企図されるようになる。

さらに作戦領域に影響を与えたのがサイバースペースの登場である。インターネットの原型とされる ARPANET は 1969 年から開発が進められた。最初のコンピュータは一室を埋め尽くすほど巨大なものだったが、1984 年にアップルがマッキントッシュを発売すると、個人が所有するコンピュータ（パーソナル・コンピュータ）の時代が始まった。そのおよそ 10 年後の 1995 年にマイクロソフトが OS ウインドウズ 95 を発売すると、一般の消費者でも電話線を介したインターネット接続が可能になり、2000 年代半ばには広帯域回線（ブロードバンド）を使ったインターネットが広く普及するようになった。パーソナル・コンピュータとインターネットの普及は、それに伴う各種の技術の標準化を促した。

そして、2007 年にスマートフォンの先駆けである iPhone をアップルが発売すると、スマートフォンを介したインターネット接続も可能になり、広く社会でサイバースペースへの接続が可能になった。

こうした機器、回線、そして標準の普及によって、重要インフラや軍事システムにおいても同様のサイバー技術が使われるようになり、RMA（Revolution in Military Affairs）の一環として捉えられた。

当然の帰結として、そうしたサイバー技術を介した軍事的な攻撃、いわゆるサイバー攻撃が登場した。2008 年頃とみられるが、中東における米軍基地の駐車場で USB メモリが意図的に落とされており、それを拾った基地関係者が基地内のパソコンにそれを挿したことで、米軍のネットワークが乗っ取られるという事態が起こった[3]。これに対処するため、米軍はバックショット・ヤンキー作戦を展開し、USB メモリに入っていたマルウェアを除去する

とともに、軍の中におけるサイバーセキュリティを高める契機とした。

2010 年に米軍で核兵器を扱う戦略軍（USSTRATCOM）の下にサイバー軍（USCYBERCOM）が設置された。サイバー軍の司令官には、インテリジェンス機関である国家安全保障局（NSA）の局長を務めていたキース・アレグザンダー（Keith Alexander）が任命された。アレグザンダーは NSA 局長とサイバー軍司令官を兼任し、こうした「ダブルハット（二重任命）」は 2023 年末時点での第 3 代サイバー軍司令官のポール・ナカソネ（Paul Nakasone）まで続いている。2024 年の早い段階で空軍のティモシー・ホーク（Timothy Haugh）が受け継ぐことになっているが、ダブルハットは続く見込みである。

NSA とサイバー軍のダブルハットは、米国議会の中では解消すべきという声もある。しかし、それが続いているのは、NSA が担うサイバースペースでのインテリジェンス活動（SIGINT）と、サイバー軍が担うサイバー攻撃および防衛の間に深いつながりがあるからであろう。

そして、陸、海、空、そして宇宙という従来の作戦領域において兵器や様々な関連システムにおいてもデジタル技術に基づくサイバーシステムに依存するようになると、ますますサイバーセキュリティが重要視された。米国に続き、各国の軍でサイバー部隊が設置され、日本でも 2014 年 3 月にサイバー防衛隊が自衛隊に設置された。

陸、海、空に続き、宇宙は第 4 の作戦領域、サイバースペースが第 5 の作戦領域という考え方は、2010 年の米軍の『4 年ごとの国防計画見直し（QDR）』で定着した[4]。そして、5 つの作戦領域を横断して作戦活動が行われなくてはいけないという認識も高まった。例えば、統合海空戦闘（joint air-sea battle）概念とは、「空と海の軍事力が全ての作戦領域―空、海、陸、宇宙、そしてサイバースペース―を横断して能力を統合し、米国の行動の自由への増大する挑戦に対処すること[5]」とされた。

2. 認知戦への注目

5 つの作戦領域を横断する戦闘、いわゆる領域横断（クロスドメイン）戦は、2018 年 12 月に閣議決定された日本の防衛計画の大綱の中心的な概念となった。それは同大綱の中では「多次元統合防衛力」と規定された。

しかし、その頃、別の作戦領域への注目が急速に始まっていた。2016 年 11 月に行われた米国大統領選挙では、その前年からロシアが様々な形で介入を始めていた。その事実は大統領選挙の結果が出るまで広く共有されることはなかったが、当然勝利すると見なされていた民主党のヒラリー・クリントン（Hillary Clinton）候補が敗れ、当初は泡沫とみられていた共和党のドナルド・トランプ（Donald Trump）候補が勝利を収めた。ロシアはフェイスブックやツイッター（現在の X）を中心に、ソーシャルメディアを通じて明らかな偽情報、あるいは、事実と偽情報を混在させる形で発信し続けた[6]。

ロシアの手法は、2014 年のロシアによるクリミア侵攻で使われた各種の手法と合わせて「ハイブリッド戦」と呼ばれた[7]。それが何を意味するのかは論者によって異なるが、一般的な共通理解は、軍事的な手段以外の手段を用いて相手国とその国民に影響を与えるということだろう。その際の影響は、物理的な打撃よりも、状況判断を誤らせたり、戦意を喪失させたりといった認知に与える影響が重視される。

こうした手法は、B・H・リデルハート（B. H. Liddell-Hart）が「間接的アプローチ」と呼んだ手法[8]や、リデルハートがベースにした孫子の兵法にもみられる考え方であり、必ずしも新しいとは言えない。しかし、リデルハートや孫子が知らなかったサイバースペースを介した認知戦は、現代ならではのものであろう。

認知戦の原型ともいえるのは、プロパガンダである。古くは紙のビラを敵陣にまき散らしたり、スパイが敵陣や敵国に入り込んで嘘を吹き込んだりすることが行われた。韓国と北朝鮮の国境地帯では、韓国から巨大な拡声器で北朝鮮政権を揺さぶるメッセージを発したり、気球を使ってビラをばら撒いたりすることも行われた。第二次世界大戦中には、ラジオ放送を使ったプロパガンダも行われた。日本軍が第二次世界大戦中に行った連合国側向けプロパガンダ放送では東京ローズとあだ名された女性アナウンサーも動員された。

現代の認知戦が新しいのは、紙や放送のように、第三者にもそれと分かる形で発せられるメッセージではなく、サイバースペースの各所にばら撒かれている情報に、多くの場合はソーシャルメディアの利用者が自分でたどり着き、それを「自分で発見した」と誤解させる点であろう。いわゆるプッシュ情報とプル情報の違いと捉えてもよいかもしれない。他者によって押しつけられた情報ではなく、他者が知らない情報に自らたどり着いたと思わせることで、その情報を強く信じさせる効果がある。その典型例が、2020 年の米国大統領選挙においてみられた Q アノン現象である。匿名掲示板への書き込みを信じる人たちが、実在しない人物の登場を強く待ちわびる様子がサイバースペース内で広く共有された。

3.ウクライナにおけるハイブリッド戦と反ハイブリッド戦

2022 年 2 月に始まったロシアによるウクライナ侵攻においては、ロシアによるハイブリッド戦が展開され、数日、長くとも数週間で帰趨が決するのではないかと考えられた。2 月 24 日にロシア地上軍による侵攻が始まるおそよ 1 ヵ月前から、サイバースペースでは各種のサイバー攻撃が展開された。それらに接していた人々は、ロシアによる物理的な侵攻も間近だと認識していた。

しかし、ロシアのハイブリッド戦はあまり大きな成果を挙げることはなかった。ロシアの手法が、2014 年とさして変わらず、古かったこともあるが、それ以上に、ウクライナ側が周到な準備をしていたことも大きい。2019 年 5 月にボロディミル・ゼレンスキー（Volodymyr Zelenskyy）が大統領に就任すると、彼の側近たちはウクライナの情報技術（IT）業界の面々

と意見交換を重ね、重要インフラ事業者との演習を何度も実施した。2014 年のクリミア侵攻で起こったことについてはおおよその対応はできていたといえるだろう[9]。

無論、戦局の展開につれ、ロシアは新しい手法を用い、ウクライナはそれに対応するということが繰り返されている。2014 年のクリミア侵攻時、ロシアの電子戦によってウクライナは状況把握のためのドローンを飛ばすことができなかったが、2022 年の侵攻以降、ウクライナは偵察用のドローンだけでなく、攻撃用のドローンも活用し、ロシアの戦力に打撃を与えている。ウクライナが用いているドローンは米国の MQ-9 リーパーのような大型のものではなく、安価で簡単に飛ばせる小型のドローンであり、戦い方を変えているといっても過言ではない。

いずれにしても、ロシアのハイブリッド戦は、所期の効果を発揮することができず、ウクライナ側の反ハイブリッド戦ともいえる戦い方が功を奏している。ということは、今後のウクライナ戦争の展開やこれから行われる紛争・戦争においては、ハイブリッド戦を超える超ハイブリッド戦が展開されることになるだろう。

2024 年 1 月の台湾総統選挙が近づく中、2023 年 12 月 26 日に演説した中国の習近平国家主席は、台湾の中国との「再統一」は「不可避」だと主張した[10]。習主席や中国人民解放軍は、ウクライナやガザの情勢をつぶさに観察し、仮に台湾侵攻を行う際に何をすべきか、急速に案を練り直していてもおかしくはない。

4. 超ハイブリッド戦

2024 年は各国で重要な選挙が行われる。主たるものとしては表 1-1 が挙げられる。70 カ国以上で 30 億人を超す有権者が重要選挙の投票用紙を手にするという[11]。これらに加え、2024 年 9 月までに日本の自由民主党の総裁任期が来るため、それに連動して日本の衆議院議員選挙も 2024 年中に行われる可能性がある。同じく英国でも 2024 年中の総選挙の可能性が高い。

表 1-1　2024 年の各国の重要選挙

時期	選挙
1 月 13 日	台湾総統選挙
2 月 14 日	インドネシア大統領選挙
3 月 17 日	ロシア大統領選挙
4 月 10 日	韓国総選挙
4～5 月	インド総選挙
6 月 6 日～9 日	欧州議会選挙
11 月 5 日	米国大統領選挙

2022 年 12 月に日本政府が閣議決定した防衛三文書のうち、国家安全保障戦略には以下の記述がある。

> 偽情報等の拡散を含め、認知領域における情報戦への対応能力を強化する。その観点から、外国による偽情報等に関する情報の集約・分析、対外発信の強化、政府外の機関との連携の強化等のための新たな体制を政府内に整備する[12]。

2023 年 4 月 14 日の記者会見で、松野博一官房長官は、外国からの偽情報に対処する体制を内閣官房で整備すると明かした。その上で、内閣情報調査室が偽情報の収集や分析を担い、首相官邸の国際広報室が対外的な発信をすると説明した[13]。総務省では 2014 年 11 月から「デジタル空間における情報流通の健全性確保の在り方に関する検討会」を開き、検討を重ねている。そうしたところ、2024 年 1 月 1 日に能登半島で地震が起こり、多くの誤情報、偽情報が広がった。4 日の記者会見で岸田文雄首相は偽情報対策について質問を受けた。首相は「SNS（交流サイト）などの事業者に対して利用規約をふまえて適正な対応をとるよう要請している。災害対策への SNS の活用については長所と短所がある」と答えた。1 月 19 日に開かれた「デジタル空間における情報流通の健全性確保の在り方に関する検討会」では、偽情報拡散防止のためのワーキンググループの設置を決めた。

2024 年 1 月の台湾総統選挙においては、様々な工作活動が行われた。与党民進党の潘孟安・総幹事長は、インタビューにおいて、以下のように発言している。

> 地方の複数の里長（日本の町内会長に相当）らが、中国当局の招待で中国大陸のツアーに参加し、野党系の候補に投票するように求められたと聞いている。高額な飲食代も負担してもらっており問題だ。台湾の司法当局が厳正に対処すると信じている[14]。

また、中国政府の国務院は 12 月 22 日、台湾産の高級魚「ハタ」の輸入を同日再開すると発表した。ハタは禁止薬品の検出などを理由に 2022 年 6 月から禁輸措置が取られていた。中国の国務院は、台湾の親中派の最大野党・国民党の要望を踏まえたと説明しており、国民党候補の侯友宜・新北市長を支援する狙いがあるとみられる[15]。

さらに、中国福建省の共産党員からの指示で、台湾総統選挙に関する世論調査のねつ造が行われたと可能性があると報じられた。12 月 20 日にメディアに公開された偽の世論調査では、野党・国民党の侯友宜候補の支持率が与党・民進党の頼清徳候補を上回っていたという[16]。

2024 年 1 月 13 日に行われた台湾総統選挙においては与党・民進党の頼清徳候補が勝利を収めた。2020 年までの総統選挙が事実上の与野党一騎打ちだったのに対し、今回は民進党に加えて、国民党の侯友宜候補、台湾民衆党の柯文哲候補による 3 人の選挙戦になった。

そのため、頼候補の獲得票数は、前回の蔡英文総統の獲得票数を大幅に下回り、立法院（議会）では過半数を失う結果になった。

それでも、中国の選挙介入が野党候補を勝たせることはなかった。介入が行われることを予期していた台湾の人々にとっては、レベルの低い偽情報は効果がなかったといえるのかもしれない。実際、インターネット上で出回った偽動画には「AI 生成」という文字が残ったままであったり、台湾では使われていない大陸の簡体字が使われていたりしたため、容易に偽情報を見抜くことができた。AI を使って高度に仕上げられた動画もあったが、あまりに発言内容が突飛だったために真実性を疑われた。TikTok 上で過激な内容のショート動画を発信していたアカウントも、あまりに似たような動画を数多く発信していたために信頼されることはなかった。

こうした例は、超ハイブリッド戦と呼ぶには十分ではない。しかし、選挙が終わった後に明らかになる、あるいは、明らかにすらならないような手の込んだ工作活動が行われていても不思議ではない。今後数年間は、新たな戦い方を考え、試し、そして実践する時期になるかもしれない。その点で極めて重要な転換点に我々はさしかかっているともいえるだろう。

日本政府は認知戦に対応した新体制をいち早く確立すべきだろう。新体制は、第一に、特定の省庁ではなく、省庁横断的な組織を中心にすべきであり、内閣官房に設置するのが適切であろう。特に、サイバー戦と組み合わせて認知戦が仕掛けられる可能性があることから、内閣サイバーセキュリティセンター（NISC）や内閣情報調査室と連携する必要がある。その際、NISC で見直しが進められている通信の秘密との整合性をとる必要もあるだろう。第二に、認知戦への対応は、サイバー戦への対応と同じく、迅速な対応が求められる。台湾政府の対応を参考にしながら、介入発見後数時間内で対応できる体制を築くべきである。第三に、認知戦は民間、それも多くは外国のプラットフォーマーを通じて行われる可能性が高いため、そうしたプラットフォーマー、ファクトチェック機関、サイバーセキュリティ企業等の官民連携の枠組みを整備する必要がある。

認知戦、特に選挙介入については 2018 年のカナダ・シャルルボワにおける G7 サミット（先進七カ国首脳会議）以来、懸念が表明され、協調的な対応が進められてきた。G7 のメンバーとなっていない欧州諸国や台湾と連携しながら、国際的な認知戦への対応を日本も進めていくべきである。

[1] Winston Churchill, *My Early Life*, London: Eland Publishing, 2002, p. 148. 日本語訳は以下より。ロバート・ゲーツ（井口耕二訳）『イラク・アフガン戦争の真実　ゲーツ元国防長官回顧録』朝日新聞出版、2015年、Kindle Location No. 4066。

[2] ジョン・L・ギャディス（五味俊樹他訳）『ロング・ピース：冷戦史の証言「核・緊張・平和」』芦書房、2003 年。

[3] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010.

[4] U.S. Department of Defense, "Quadrennial Defense Review Report," U.S. Department of Defense, February 2010, (accessed on January 2, 2024).
<https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf>

[5] ibid., p. 32.

[6] 以下などを参照。土屋大洋、川口貴久編『ハックされる民主主義：デジタル社会の選挙干渉リスク』千倉書房、2022 年。小泉悠、楽原響子、小宮山功一朗『偽情報戦争：あなたの頭の中で起こる戦い』ウェッジ、2023 年。

[7] 本報告書の第 2 章を参照。以下などを参照。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。佐々木孝博『近未来戦の核心サイバー戦―情報大国ロシアの全貌―』扶桑社、2021年。

[8] B・H・リデルハート（市川良一訳）『リデルハート戦略論―間接的アプローチ―』原書房、2010 年。

[9] 秋田浩之「ゼレンスキー氏からの伝言　有事に耐えられるインフラを」『日本経済新聞』2023 年 12 月 25 日電子版。

[10] 「習氏、台湾の『再統一』は『不可避』　総統選迫る中で主張」CNN、2023 年 12 月 27 日（2023 年 12 月 29 日アクセス）。<https://www.cnn.co.jp/world/35213297.html>

[11] 「史上最大の選挙イヤー　トランプ劇場、再来の危機」『日本経済新聞』2023 年 12 月 27 日電子版。

[12] 国家安全保障会議「国家安全保障戦略」2022 年 12 月 16 日、24 頁。
<https://www.mod.go.jp/j/policy/agenda/guideline/pdf/security_strategy.pdf>

[13] 「偽情報への対策強化　内閣官房で体制整備」『日本経済新聞』2023 年 4 月 14 日電子版。

[14] 「どうなる台湾総統選、終盤戦へ 各党の選挙参謀に聞く」『日本経済新聞』2023 年 12 月 15 日電子版。

[15] 「中国、台湾産高級魚の輸入再開　総統選にらみ野党支援か」『日本経済新聞』2023 年 12 月 22 日電子版。

[16] 「台湾総統選めぐり"中国側の指示で世論調査を捏造か"摘発相次ぐ」TBS News Dig2023 年 12 月 26 日（2024 年 1 月 1 日アクセス）。<https://www.youtube.com/watch?v=FfgvQHA4z2w>

第２章
ロシア流の戦争と中露安全保障協力

佐々木 孝博

はじめに

2022 年 2 月 24 日にウクライナ戦争が勃発してから約２年が経過し、各種の教訓が次第に明らかになってきた。特に、目に見えないところで行われていたサイバー戦、情報戦、宇宙領域および電磁波領域の戦い、AI を駆使した戦いなどと物理的な領域での戦いを融合した全領域戦とも言える戦い方の全容が判明してきた。そこで本章においては、まず、「ロシア流の戦争」としてロシアが志向する「全領域での戦い」というものを、各種戦略文書に大きく影響を及ぼしたヴァレリー・ゲラシモフ（Valery Gerasimov）参謀総長の戦略論文を中心に考察していく。そして、ウクライナ戦争を通じて明らかになってきた「全領域戦」を、特に目に見えないところで行われていた「AI を駆使した戦い」、「情報空間・サイバー空間、電磁波領域、宇宙領域における戦い」などに焦点を当て考察していく。その過程で露呈してきたロシアの戦略の欠点・課題についても考察していきたい。最後に、台湾有事の観点から、中露の安全保障協力の今後についても考えてみたい。

1.全領域での戦いを重視するロシアの現代戦

2014 年のロシアによるクリミア併合の事例や 2016 年の米国大統領選挙への介入事例などを考察して、ロシアによる「新たな世代の戦い（現代戦）」を、非軍事手段を中心に行う戦略と捉える先行研究が多くなってきた。いわゆる「ハイブリッド戦」という戦い方である。

ロシアが現代戦で重視するのは、2013 年に発表したゲラシモフ参謀総長による戦略論文「先見の明における軍事学の価値（正確にはゲラシモフが軍事学アカデミーで行った講話の講話録）」によれば、平時から低列度紛争までの段階においては、各種プロパガンダ活動、

SNS による情報の流布、フェイクニュースの拡散、戦略的な情報リークなどにより情報戦を行い、対象国の政権を打倒し、対象国に親ロシアの政党や世論を形成させ、対象国をロシアの影響下に置くという、非軍事手段を重視した戦い方を行う。これによって、一義的には「戦わずして勝つ」、「軍事力を行使した際にも圧倒的に有利な情勢を作為する」といった戦略を採る。

非軍事手段のみで目的が達成できない場合は、物理的な軍事力も行使する。その際は、陸、海、空、宇宙、サイバー・情報空間、電磁波領域などあらゆる領域の全縦深であらゆる軍種を活用した軍事行動を行う。その際、ハイテク兵器、民間軍事会社、正規軍・非正規軍、特殊部隊などあらゆる軍事手段を融合させ実施する。さらに、あらゆる戦い方（正規戦・非正規戦、情報戦・サイバー戦、電磁スペクトラム戦、対称戦・非対称戦、物理的な接触戦・非接触戦など）を採用する。

換言すると、非軍事・軍事の考え得るあらゆる手段、あらゆる組織、あらゆる戦い方を融合させたという意味での「ハイブリッド戦」という戦い方である。ゲラシモフ参謀総長によれば、低列度紛争においては、非軍事と軍事の割合は 4：1 であり、非軍事手段による戦略をより重視しているということである。

2.ウクライナ戦争で実践された全領域戦

（1）AI を駆使した指揮統制・作戦指揮

前項でも触れたように、あらゆる手段であらゆる領域で戦うことを重視するロシアでは、近年、特に AI を活用し世界でも抜きんでた軍事力を構築しようとしている。しかしながら、準備不十分のため、ウクライナ戦争では間に合わなかったとみられている。

それに比較して、弱者の戦い方を追求しているウクライナでは、米国をはじめ西側諸国の支援も得つつ AI を駆使した指揮統制を実施していることが徐々に明らかになってきた（図 2-1 参照）。ウクライナが利用した最大の AI は、米国パランティア社が提供した「AI プラットフォーム」を利用した戦略指揮・作戦指揮である。パランティア社では、ウクライナ政府に AI プラットフォームというものを提供し、戦略指揮・作戦指揮に活用しているということが同社のアレックス・カープ（Alexander Karp）最高経営責任者（CEO）のインタビューにより明らかとなった。この AI プラットフォームには、西側諸国から提供された偵察衛星による情報や早期警戒機が入手した情報に加え、ウクライナ軍が独自に入手した戦場の情報や市民から通報されたロシア軍の動静に関する情報などが入力されているということである。これらの入力情報をパランティア社独自のアルゴリズムで AI により解析・分析し、1 日当たり 300 の目標を選定し、複数の作戦を指揮官に提供する能力があるとのことである[1]。

ウクライナ軍は戦争の経験がロシア軍に比して少ないという欠点を、AI を活用することにより、逆にロシア軍を凌駕するレベルにまで引き上げ、弱者が強者に勝つための戦いを行っていると評価できるだろう。

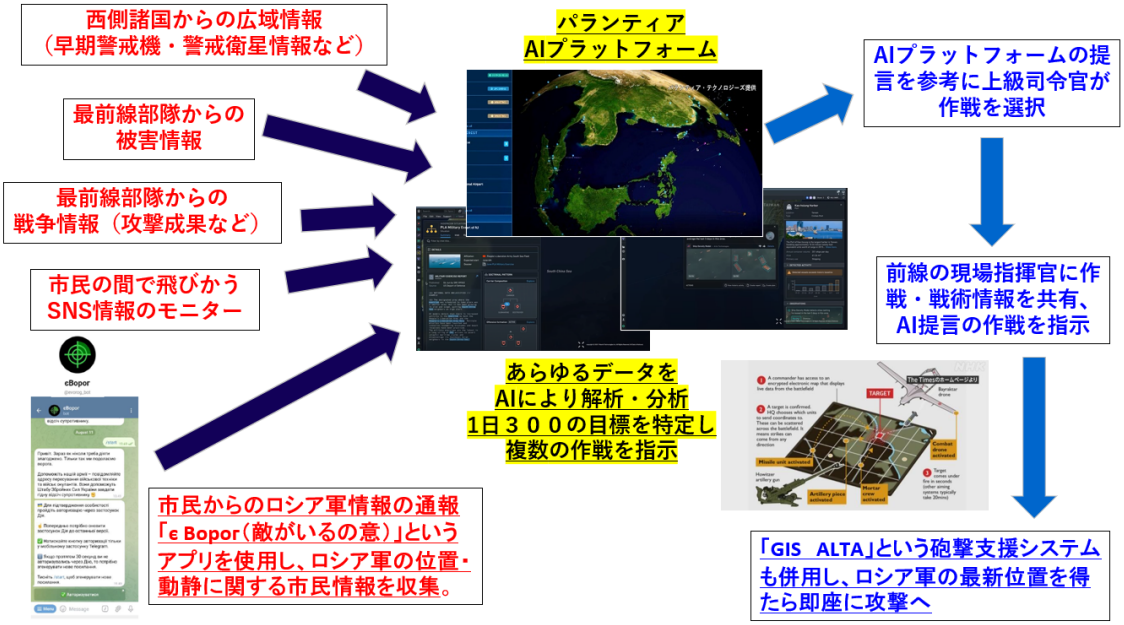

図 2-1　AI プラットフォームを活用したウクライナ軍の指揮統制

出典：BS-TBS「報道 1930（2023 年 2 月 7 日放送）」、パランティア社広報動画等から作成。

（2）ウクライナ戦争における情報戦

2022 年 6 月に米国マイクロソフト社が発表した分析レポートは、ウクライナにおけるロシアによる影響工作には 4 つのターゲットがあったことを指摘している[2]。

第 1 は、ロシア国内である。その目的は、いわゆる「特別軍事作戦」の支持、政権支持の維持などである。国内の支持基盤は未だ崩れていないことから、国内をターゲットとした情報戦に関しては、ほぼ意図どおりに目的は達成していると言えるだろう。

第 2 は、ウクライナ国内である。その目的は、ロシアの軍事侵攻に抵抗するウクライナ国民の継戦意思を挫くこと、そして、でき得るならば、親ロシアの世論を形成させて親ロシア政権を樹立することである。2014 年のクリミア併合時には、親ロシアの世論が形成され、表面上、民意のもとに併合が達成されたことから一定の成果を得ていたが、今回は、ウクライナ国民の民意は反ロシアとなっており、ほぼ失敗していると言えるだろう。その大きな要因は、ロシア側が発信する偽情報に対し、ファクトチェックができる体制が構築されていること、及び国民が偽情報に簡単には惑わされない情報リテラシーが高いことにある。

第 3 のターゲットは米国や欧州を中心とした西側諸国である。その目的は、特に米英と

大陸ヨーロッパ国（独仏など）との分断を図り、西側諸国の結束を弱め、一体となった制裁やウクライナ支援を阻止することにある。クリミア併合時には、ドイツをはじめ一定の国はロシアからのエネルギーに依存しており、ロシアとしては限定的な成果は得たと考えられるが、今回はほぼ失敗している。この分野では、ボロディミル・ゼレンスキー（Volodymyr Zelenskyy）大統領が各国議会で行ったスピーチをはじめとするウクライナによる戦略的な情報発信がロシアのプロパガンダよりも効果を上げていると評価できるであろう。

第 4 のターゲットは、西側諸国以外の国際社会である。2014 年のクリミア併合時も今回も国際社会は、ロシアの制裁に賛同するグループ、ロシアにエネルギーや食糧などを依存しており、一定の理解または忖度するグループ、及び各々の国益に鑑み中立を維持するグループの 3 つに分かれている。この分野の情報戦では、ロシアは一定の成果を得ていると言えるだろう。

（3）電磁波領域での戦い

今回の戦争における侵攻当初、ロシアは保有する強力な電子戦装備を積極的に活用してこなかった。この理由は、米国の電子戦専門家ブライアン・クラーク（Bryan Clark）の分析などを総括すれば、以下のことが導き出せる[3]。

第 1 は、ロシアの電子戦部隊は、クリミア併合以降ウクライナ東部地域で行ってきたように、無線と携帯電話を傍受してウクライナ軍の位置を特定するために、「レール 3」という電子戦兵器を使用した。しかし、住民が過疎なウクライナ東部と人口が密集している首都キーウ近郊は戦略環境が全く異なっている。キーウ近郊では、民間と軍事の通信が混在しているので、ロシア軍はウクライナ軍の位置を特定できなかったのではないかということだ。

第 2 は、ウクライナ軍が NATO の秘匿通信系「SINCGARS」を使用し始めたことが、ロシア軍による電子戦が活発でなかった要因と考えられるということだ。ロシアの現有の電子戦装備では周波数ホッピング方式を使う「SINCGARS」を使った軍事通信は探知することが困難であったとみられる。

第 3 は、キーウへの進軍では、ロシアの電子戦装備が大型であり、進軍しながらの運用には適していなかったことも、侵攻当初、電子戦が低調であった要因の 1 つと考えられている。

したがって、東部に作戦領域が移ってからは、ドンバス地方の前線が短期間には移動しないので、電子戦装備を一ヶ所に固定し、そこから運用していることが電子戦装備を多用している要因ではないかとみられる。

（4）宇宙領域での戦い

今次戦争では、ロシア国内での GPS 干渉についても観測されている。2022 年 12 月 5 日、サラトフ地域のエンゲルス 2 基地とリャザン近郊のディアギレヴォの 2 つのロシア空軍基地がウクライナのドローンにより攻撃された。その 6 日後、GPS の干渉状況を監視している組織『GPSJam.org』によれば、エンゲルス 2 空軍基地付近での干渉が大幅に増加し、マ

リニコワ空軍基地周辺で新たな干渉がみられた。また首都モスクワ近郊でも GPS 干渉が観測されている（図 2 -2 参照）[4]。

GPS 干渉により、ロシアは、GPS データに基づいて誘導しているウクライナによる UAV の攻撃から、重要な基地及び首都モスクワを防護しているということだ[5]。

加えて、2023 年 5 月 6 日、米 CNN によれば、米供与の高機動ロケット砲システム「ハイマース」がロシアによる電子妨害によって精度が低下し、ウクライナ軍が対策を強いられている旨が報じられた。ロシア軍は、電子妨害により「ハイマース」の GPS 誘導を狂わせ、ウクライナ軍の使用するロケット弾の目標精度を低下させているとのことである[6]。この事例も、GPS 干渉による電子妨害が効果を示している一端と言えるだろう。

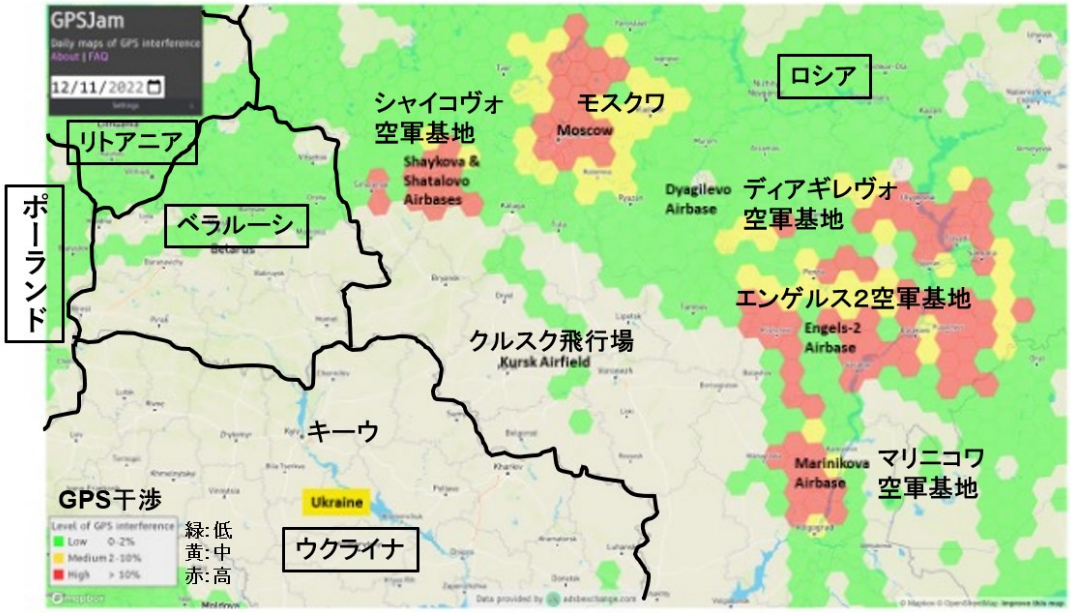

図 2-2　GPS 妨害の状況

出典：GPS World, Ukraine attacks changed Russian GPS jamming,を基に作成。

3. 中露の安全保障戦略と安全保障協力

（1）中国の「超限戦」を研究したロシアの「全領域戦」

1999 年、中国人民解放軍（PLA）の現役将校 2 人（喬良大佐及び王湘穂大佐）が「超限戦」という戦略論文を発表した。その主たる内容は、「超限戦」の名のとおり、21 世紀の戦争は、「あらゆる限度を超えた紛争」であり、「あらゆる手段が軍事兵器になり、あらゆる場所で軍事紛争が生起する」といったことであった。すなわち、軍事・非軍事手段、正規・非正規組織、作戦領域などを問わず、あらゆる制限や制約を超えて国家目標を達成するとの戦

略である。

時系列から考察すると、ロシアはこの中国の超限戦を研究し、自国戦略に活用した可能性が非常に高い。冒頭触れたゲラシモフ論文においては、情報空間における国家転覆活動の脅威を念頭にして、「21 世紀においては、平和と戦争の間の多様な摩擦の傾向が続いている。戦争はもはや宣言するものではなく、我々に馴染んだ形式の枠外で始まり進行するものである。(中略) もちろん、『アラブの春』は戦争ではなく、我々軍人が研究しなくてもよいというのは簡単である。しかしながら、これが 21 世紀の典型的な戦争ではないだろうか」と冒頭で述べている。まさに、あらゆる手段を用いるという「超限戦」で記述された内容を、現在のロシアに適用したものと言えるだろう。したがって、ロシアの「全領域戦」と中国の「超限戦」は、その目的・手法等において非常に類似しているということである（図 2-1 参照)。

図 2-1　中国の「超限戦」とロシアの「全領域戦」のイメージ

中国『超限戦』角川新書（２０５頁から引用）

軍事	超軍事	非軍事
核戦争	外交戦	金融戦
通常戦	インターネット戦	貿易戦
生物・化学戦	情報戦	資源戦
生態戦	心理戦	経済援助戦
宇宙戦	技術戦	法規戦
電子戦	密輸戦	制裁戦
ゲリラ戦	麻薬戦	メディア戦
テロ戦	模擬戦（威嚇戦）	イデオロギー戦

ロシア『全領域戦』（各種戦略文書から筆者作成）

軍事	軍事＋非軍事	非軍事
核戦争	情報戦	金融戦
通常戦	サイバー戦	貿易戦
生物・化学戦	電磁波戦	資源戦
宇宙戦	心理戦	外交戦
テロ戦	非対称戦 非接触戦	法律戦
ゲリラ戦	技術戦	制裁戦
	制脳戦	メディア戦
	ＡＩ戦	イデオロギー戦

出典：渡部、佐々木『現代戦争論－超「超限戦」』等を基に作成。

（2）ウクライナ情勢と台湾情勢の相違[7]

陸上作戦が主体のウクライナ戦争と海上作戦・航空作戦が主体の台湾有事

ウクライナ戦争では長大な国境を接する隣国同士の戦いであるため、当然、陸上作戦が主体となっている。そのため、陸上兵力を侵攻させるとともに、兵員や装備の陸上輸送などのロジスティックスが勝敗に重要な位置を占める。

一方、台湾有事が生起するとすれば、島国に対する軍事侵攻であるために、当然、海上作戦や航空作戦が重要な位置を占めることになる。ウクライナ戦争では、陸上戦力の侵攻ルートに関連する地形や河川、泥濘など、地形上の障害が重要となっていた。台湾侵攻では陸海

空兵力を融合した上陸部隊が如何に着上陸できるか、上陸後は海上における補給ルートが如何に確保できるかが重要になってくる。民間人の避退まで考慮すると、ウクライナ戦争ではロシア軍の脅威とは反対方向のヨーロッパ方面へは簡単に退避できる状況にはあったが、台湾有事では、民間人の避退は海上ルートを介さなければならず容易ではない。退避ルートの話は、軍事物資の補給ルートにも直結しており、ウクライナ戦争では、同盟国・同志国からの支援は比較的容易に行えるが、台湾有事では海上輸送を介さなければならず、水中からの脅威も考慮しなければならないので、その困難性は増す。

総じていえば、「今日のウクライナ有事は、明日の台湾有事」ともいわれるが、両者の安全保障環境は全く異なっており、台湾有事はウクライナ戦争に比して、攻撃も防御もどちらも難しい環境にあると言えるだろう。

情報戦・サイバー戦が軍事侵攻前に激化

前項では実戦闘での相違について述べたが、物理的な戦闘に移行する前の段階においては非常に類似している側面もある。それはロシアにとってのウクライナ、中国にとっての台湾はともに民族は同系統で使用言語も同系統であり、文化的に非常に類似しているということだ。民族や使用言語が同系統ということは、ロシアによる全領域戦や中国による超限戦でも重視される非軍事手段の情報戦やサイバー戦が比較的容易かつ効果的に実施できるということである。

したがって、物理的な実戦闘の段階に移行する前に、情報戦やサイバー戦といった非軍事手段による侵略が激化するという側面において両者は非常に類似していると言えるだろう。中国もでき得るならば、物理的な軍事侵攻に至る前の段階で、台湾に親中国の政権を確立させ、合法的な手段で血を流さずに併合できてしまえば長年の国家目的で習近平政権の悲願である台湾統一は成し遂げられるということである。そういった面から 2014 年のロシアによるクリミア併合は、中国に数多くの示唆を与えていたものと推察される。

ロシアと同様な欠点をもつ中国の指揮統制

指揮統制の類似性についても指摘したい。ロシアは旧態依然の「命令による指揮（中央が全てを決定し、最前線の部隊まで統制する指揮）[8]」を重視し、指揮統制が硬直化しており、情勢の変化に柔軟に対応できていないという欠点を有している。さらに現代戦におけるカギとなっている統合作戦（各軍種の融合）、統合指揮統制についても、正規軍、非正規軍が入り乱れた軍事作戦を行っているために統制がとれていないという欠陥も有している。実は、同種の欠陥は中国人民解放軍（PLA）ももっているのではないかということを指摘したい。

PLA も旧ソ連軍と同様に命令による厳格な指揮統制を有しているとみられ、中央統制を強化するために中国共産党の政治将校的な配置も維持しているものとみられている。したがって、現在のロシアよりもさらに硬直化した指揮統制体制にあるのではないかと考えら

れる。さらに各軍種を融合した統合指揮というものも、全領域戦を実体験として経験していない PLA にとっては未知の領域と考えられる。統合指揮統制の難しさは、米軍をはじめ西側各国も痛感しており、その是正に長年尽力しているが、時間がかかっている。この面でも、西側諸国と比較して PLA はロシア同様一歩遅れているとの感がある。

ロシアが失敗したロジスティックス（後方・兵站）は中国も同様

PLA は、ロシア軍（旧ソ連軍）から様々な軍事装備を導入してきた経緯から、ロジスティックスに関してもロシア同様の問題点があるものと考えられる。それは、「プッシュ型兵站」と「プル型兵站」の問題である。ロシア軍では旧ソ連軍以来、中央が作戦指揮を現場指揮に至るまで細部にまで詳細に行っており、それが中央統制によるプッシュ型兵站につながっている。中央が考える最適な補給支援を中央の指揮通りに、中央からのプッシュ体制として実施している。この方法では、現代戦における複雑な戦況の変化に十分に対応できる兵站体制とは言えず、西側諸国では、現場が必要な補給支援物資を現場から中央に進言し、中央ではそれに基づき最適な補給ルートを選定し、現場が真に必要とする物資を適時適切に現場に行きわたらせるといったプル型兵站を行っている。PLA もプル型兵站体制に移行できないと、ロシアと同じような失敗を重ねる可能性が高い。

ウクライナ戦争の教訓解決まで軍事侵攻に踏み切る可能性は低い

本項で言及してきたウクライナ戦争で露呈したロシア軍のもつ欠陥や問題点は PLA も同じように保有しているとみられ、それが解消できなければ、中国も台湾への軍事侵攻を簡単には決心できないのではないかとみられる。中国の台湾侵攻があるとすれば、その可能性として 2027 年（PLA 創立 100 周年）がよく挙げられるが、少なくとも政治的な要件の制約がないそれ以前の段階での実行は難しいのではないかと考えられる。それまでは、軍事侵攻の決断よりも、考え得るあらゆる非軍事手段を駆使して台湾の世論を動かし、親中国の政権の確立を企図し、非軍事による台湾統一を目指すのではないだろうか。

2023 年 1 月 9 日に米国のシンクタンク「戦略国際問題研究所（CSIS）」が台湾有事のシミュレーションを実施した結果を発表したが、2 つの条件以外は中国による台湾への軍事侵攻は失敗するとの結果を導き出している[9]。中国が台湾侵攻を成功させる 2 つの条件とは、「米国が関与せず、台湾独力での対応となった場合」と「日本が中国の圧力に屈し、在日米軍基地の使用などで米軍を支援しなかった場合」である。そのような観点からすると、我が国における日米同盟に対する否定的な世論形成や米国における台湾関与に関する否定的な世論形成のための情報戦を考慮しておくことにも注視していかなければならないだろう。

（3）中露安全保障協力の見積もり

最後に、ウクライナ戦争を経て、台湾有事の観点からロシアと中国がどこまで安全保障協力を進めるかについても見ていきたい。

中露の安全保障関係は、歴史的にみると、米国を含めた 3 国関係を考察していかなければならないだろう。つまり、米中の関係が良好な時は中露の関係は疎遠になり、米中の関係が険悪になれば、中露関係は良好になるということである。2018 年 10 月当時のマイク・ペンス（Mike Pence）米副大統領の演説以降、米中は覇権争い時代に突入したと考えられ、中期的に見てこの関係（対立）は継続するものと見積もられる。そのような情勢の中では、中露関係はより緊密になってしまうということである。

2023 年 3 月 21 日、習近平国家主席は、ウクライナ戦争の最中、ロシアを訪問しウラジーミル・プーチン（Vladimir Putin）大統領と会談した。報道によれば、両国首脳は中露関係及び関心を共有する重大な国際・地域問題について会談を行い、多くの新しい重要な共通認識に至り、また、新しい時代の包括的・戦略的（協力）パートナーシップを深めることで合意したとのことである。特に会談後、プーチン大統領からは、「ロシアは、台湾地区、香港特別行政区、新疆ウイグル自治区関連の問題において中国が自らの正当な利益を守ることを断固として支持する。中国との国際協力を一層緊密化していきたい」との発言があり、台湾問題に対するロシアの支持を明確にした。

中露の関係は首脳間の発言では「同盟」の言葉も度々使用されているが、正確には「戦略的パートナーシップ」の関係と位置付けられている。すなわち、国益に合致する戦略分野では協力する、個々の領域では是々非々で対応するといった関係である。米国という中露両国にとっての共通の脅威には一致して対抗するといった関係である。したがって、台湾有事は米国という共通の脅威への対抗という文脈で協力を深化させる分野であるとは位置づけられるだろう。ただし、軍事協力の詳細については、ウクライナ戦争の裏返しであり、台湾有事に際してのロシアの協力は国益をみて限定的になるものと見積もられる。直接の軍事協力というよりは、中国が仮に軍事行動を判断した場合には、ロシアに対しては、同時に日本海などで大規模な演習や戦略爆撃機による我が国周辺の威嚇飛行など日米の兵力を分散させるための行動を期待するものと考えられる。

おわりに

ロシアが志向する「全領域での戦いを重視する現代戦」というものを、各種戦略文書を中心に考察してきた。ロシアによる「全領域戦」とは、非軍事・軍事のあらゆる手段、あらゆる組織、あらゆる戦い方を融合させたという意味での「ハイブリッド戦」という戦い方である。

今次のウクライナ戦争では、ロシア・ウクライナ双方とも、特に目に見えないところで「AI を駆使した戦い」、「情報空間・サイバー空間、電磁波領域、宇宙領域を駆使した戦い」など、「全領域戦」とも言える戦いを実行に移していた。そこには、成功した例、失敗した例双方の教訓があった。

ウクライナ戦争におけるロシアの失敗の教訓を横目で見つつ、台湾統一を目指す中国も、ロシアの「全領域戦」と類似の「超限戦」という戦略を保有している。併せてロシアが今次戦争で失敗した類似の問題点も保有しているとみられる。それらの教訓から得られた問題点を解決できなければ、中国は台湾への軍事手段を使った統一には踏み切れず、それまでは、情報戦を中心とした非軍事手段により台湾統一を目指していくものと見積もられる。さらに、中露の安全保障関係は、米国という共通の脅威には一致して対抗するといった関係にとどまるため、台湾有事に際してのロシアの協力は、ウクライナ戦争の裏返しであり、国益をみて限定的になると考えられる。

---

[1] パランティア社広報動画 <https://www.youtube.com/watch?v=-kjYQ8q9IYY>

[2] Microsoft, Defending Ukraine: Early Lessons from the Cyber War, June 22, 2022. <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>

[3] Bryan Clark, "The Fall and Rise of Russian Electronic Warfare", Hudson Institute, July 30, 2022. <https://www.hudson.org/research/18018-the-fall-and-rise-of-russian-electronic-warfare>

[4] GPS World, Ukraine attacks changed Russian GPS jamming, December 22, 2022. <https://www.gpsworld.com/ukraine-attacks-changed-russian-gps-jamming/>

[5] David Hambling「『偽衛星信号』でロシアのドローンを誤誘導、ウクライナの新たな電子戦が奏功」Forbes、2023 年 4 月 27 日。 <https://forbesjapan.com/articles/detail/62792>

[6] CNN, Russia's jamming of US-provided rocket systems complicates Ukraine's war effort, May 6, 2023. <https://edition.cnn.com/2023/05/05/politics/russia-jamming-himars-rockets-ukraine/index.html>

[7] この項、渡部悦和、佐々木孝博ほか『プーチンの「超限戦」: その全貌と失敗の本質』ワニブックス、2022 年を参考としている。

[8] これに対し、西側諸国では変化する情勢に柔軟に対応するため「任務による指揮（上級指揮官は最前線に対し任務のみ付与し、実施の詳細は現場指揮官に任せる指揮）」を実施している。

[9] Mark F. Cancian, Matthew Cancian, and Eric Heginbotham, The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan, Center for Strategic and International Studies (CSIS), January 9, 2023. <https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan>

第３章
中国は何を学んでいるか

八塚 正晃

はじめに

ウクライナ戦争は、伝統的な火力のみならずサイバー、宇宙、さらには認知領域を含む多岐にわたる領域で戦闘が行われ、さらには、域外国や非国家主体が関与して戦争の行方に影響を与えている。このため、多くの国家が同戦争を様々な角度から検証し、今後の自国の軍事作戦に対する教訓を引き出そうとしている。当然ながら、教訓とは自ら置かれた環境に基づいて引き出されるものである。中国の場合、東アジア情勢、とりわけ台湾海峡における軍事力行使を含む統一工作がそれに当たろう。

本章は、こうした問題意識を念頭に置き、中国国内で発表されている論考を手掛かりにして、中国がウクライナ戦争をどのように評価し、いかなる教訓を引き出しているかを析出することを試みる。とりわけ、中国軍関係者や専門家らの宇宙、サイバー、認知などの領域の戦いに対する評価に注目しつつ、今後の中国人民解放軍の軍隊建設の方向性についての示唆を検討したい。

1.“ハイブリッド”な戦争と国際化

ウクライナ戦争についての中国国内における議論を見ると、日本におけるそれと同様に、世界有数の軍事大国であるロシアに対してウクライナが善戦しているとの評価が広くみられる。とくに中国の研究者らの関心事項は、なぜ軍事力で劣勢にあるはずのウクライナが軍事大国のロシアにこれだけ有効に対抗できているのか、という点にある。もちろん、この理由をウクライナ軍の士気の高さや作戦能力に求める見方もある。中国人民解放軍軍事科学院の趙小卓研究員は 2023 年 2 月に発表した論文で、今回の戦争は「機械化戦

争と情報化戦争の二種類の戦争形態の勝負となっている」と指摘したうえで、ウクライナ軍は作戦理念、作戦方式、組織形式の点で情報化戦争を実施している一方で、ロシアは第二の軍事強国と言われるものの戦場で投入される武器装備は先端的なものが少なく、作戦理念や実施は機械化戦争の痕跡を深く残しているとして、オペレーショナルな観点からウクライナ軍の戦い方に高い評価を与えている[1]。なお、中国人民解放軍は、従来型の戦争が物質とエネルギーを用いて敵を人的・物的に破壊することで勝利を得る「機械化戦争」であったのに対して、現代の戦争は、高度な情報運用能力を活用することで効率的な統合作戦を実施したり、サイバー攻撃などを通じて非物理的に敵の指揮命令系統を麻痺させたりすることなどを中心とした「情報化戦争」になっているとの見解を示している。

他方で、中国国内の議論の特徴的な点として、ウクライナ戦争の「ハイブリッド」な側面にもかなりの程度注目していることがあげられる。ロシアによるウクライナ侵攻から一年以上経た 2023 年 5 月に汪海江・西部戦区司令員は、「ウクライナ危機は、勃発後に“ハイブリッド戦争”の新たな形態を露わにし、軍事戦・政治戦・金融戦・科学技術戦・サイバー戦・認知戦がそれぞれ交錯しつつ、戦争における争いが伝統的な領域から非伝統的な領域にまで延伸し、総合国力、戦争潜在力、軍事力の全面的な力比べになっている」と指摘する[2]。ロシア軍がこれまでの紛争で発展させてきた「ハイブリッド戦争」を今回のウクライナ戦争でいかに実施するか、という問題意識を他国の軍幹部が持つこと自体は自然なことであろう。今回のウクライナ戦争では「ゲラシモフ・ドクトリン」を提起したヴァレリー・ゲラシモフ（Valery Gerasimov）総参謀総長が一時期総司令官として指揮を取っていたことを考えれば尚更であろう[3]。興味深いことは、中国国内の議論では、今回のウクライナ戦争が「ハイブリッド」であることこそが、ロシア軍をして苦戦させている要素として論じられていることである。

ウクライナ戦争がハイブリッドな性質を持つことで、いくつか重要な側面をもたらしている。その一つが紛争の国際化である。今回の戦争は一義的にはウクライナとロシアの二国間紛争であるが、他方で、NATO を中心とした西側諸国がウクライナに対して武器装備の提供・軍事訓練・財政支援など幅広い側面から間接的に関与している。中国の論者の多くが、こうした側面に注目して、ウクライナ戦争を「代理戦争」と評価している[4]。例えば、ウクライナ戦争の一周年を振り返る『解放軍報』の特集記事は、「米国と西側諸国は、この紛争を利用して、ロシアに対する政治的批判・包括的な外交圧力・文化的孤立を試みており、ハイブリッド戦争の手法によって総力戦を実施し、経済的・技術的な優位性を利用して制裁という大鉈を振るい、戦略的な絞殺を試みている」と指摘する[5]。すなわち、西側諸国は、ウクライナ領内でロシアと戦火を交えるような直接的な軍事介入を否定しているものの、多種多様な形でウクライナを支援することで、ウクライナをして大国ロシアへの善戦を可能とさせているとみている。この関与が、サイバー・宇宙・認知など非物理領域や、武器支援のみならず財政支援・対ロ経済制裁・外交工作など非軍事的な形でなされていることこそが、ウクライナ戦争をハイブリッド戦争たらしめているというわけ

である。言い換えれば、ウクライナ戦争の緒戦において、ロシアによる侵攻を効果的に押しとどめたのは、携行式の対戦車ミサイル「ジャベリン」や対空ミサイル「スティンガー」などの米国などから提供された装備であることに異論はないであろう。また、NATOの偵察機がポーランド・ルーマニア・黒海の上空を飛行しつつ、衛星監視・海上偵察などで戦場の情報をウクライナへ継続的に提供した。さらに、こうした軍事支援のみならず、ロシアに対する経済金融制裁、外交的圧力をかけることがロシアの総合的国力を削っている。こうした紛争の国際化による効果に対して、中国の軍関係者らは警戒感をもって注視している。

2.民間企業の関与、民生技術の活用

ウクライナ戦争では、国家主体だけでなく民間企業や個人などの非国家主体も戦争に参画しており、民間企業が提供する民生技術を利用した武器装備が大量に投入されていることも注目される。こうした民間企業が提供する技術は、特に宇宙・サイバー・認知領域において大きな役割を果たしている。国家主体と比べて、民間企業や個人などの非国家主体は、必ずしも国家間のルールや各種制約を受けることもないため、その戦略や戦術について多元的に選択可能である[6]。これは、中国との関係で考えた場合、「一つの中国」原則などに縛られないことを意味する。総合国力が劣勢のウクライナ側にとっては、非国家主体を通じた挑発、動員、消耗戦などの非対称な戦いを仕掛けることによって、優勢な相手に有利な戦いを展開することが可能となる。シスコやマイクロソフトなどの米国の情報技術企業は、ウクライナに対してサイバー脅威情報や防御に関するアドバイスを提供したとされる。また、ウクライナ戦争においてはハッカーらによる自発的なサイバー攻撃も活発にみられたが、これは中国においては NATO による世論戦が功を奏した結果と評価される。中国の情報技術企業である北京知道創宇信息技術股份公司の研究者らは、「NATO は直接的に軍事関与をしないといいつつも、国際制度を主導するとともにメディア・プラットフォームを武器化し、ロシアへの圧力を最大化し、自らのサイバー優勢を利用して、ハッカーたちをウクライナ戦争に招き入れた」と指摘している[7]。

民間企業の関与の中でも、とりわけ注目されるのが、イーロン・マスク（Elon Musk）が提供したスターリンクである。中国においてはウクライナ戦争以前から、スターリンク衛星による低軌道コンステレーションが通信・偵察・早期警戒の分野において軍事利用される可能性について注目されていた[8]。

中国人民解放軍の研究者らは、実際のウクライナ戦争でも、スターリンクが安定的かつ継続的なネットワーク通信を提供することで、地上作戦、精密打撃、無人機運用、対ネットワーク電子妨害などの側面でウクライナ軍の能力を強化していると分析している[9]。また、ウクライナ軍によるスターリンクの利用は、戦争をより複雑にさせていると中国軍関

係者は捉える[10]。すなわち、米軍も利用するスターリンクのシステムに対してロシア側が攻撃を加えることは、米国に対する攻撃を意味し、戦場の宇宙空間への拡大や戦争のエスカレーションを招くリスクがあるという。つまり、ウクライナによる米国資本の利用が、ロシアのエスカレーション管理の計算を複雑にし、作戦選択に制約を課したことを意味する。

既に明らかになっているように、イーロン・マスクは、ウクライナによる南部クリミアのロシア海軍艦隊への奇襲攻撃を妨害するためにスターリンクの接続を切るなどしており、必ずしもウクライナに対する一貫した支援をしているわけではない。他方で、企業等に対する政府権力が強い中国においては、中国の識者らは、米国企業と米国政府・軍の一体性を当然視する傾向にある。スターリンク衛星の発射場の一部が米国のヴァンデンバーグ空軍基地に建設されたことや、米陸軍と軍用ネットワーク間における伝送システムに関する契約を結んだこと、米空軍から資金提供を受けて戦闘機との暗号化された相互接続実験を実施したこと等を挙げ、スペースXが米軍との密接な関係にあると彼らは評価するのである[11]。

スターリンクの戦場への登場は、その対応策についての検討を中国の軍事関係者らに促している[12]。四川省軍区データ情報室の関係者らは、スターリンクは、将来の戦争においてますます重要な役割を果たす可能性があり、スターリンクの脅威にどう対処するかを研究する必要がある、と提起する[13]。具体的には、スターリンクが展開する低軌道において、中国のコンステレーション衛星構築の計画を加速させ、周波数資源や軌道資源を確保し、戦略的高地を掌握するよう主張する。彼らは特に、低軌道衛星コンステレーションが無人機の作戦に与える影響について注目し、①地上の標的に対するグローバルかつリアルタイムな偵察を実施することができ、作戦制御・状況認識・情報共有・ターゲティングの高度化が可能となる、②地上・海上・空中の無人機による「非接触」の長距離精密打撃を実現できる、③安定した通信を保証することにより無人機のスウォーム運用が可能となる等と指摘する[14]。

3.認知領域における戦い

今回のウクライナ戦争では熾烈な世論戦が展開された。紛争行為の正当性をめぐって、様々なナラティブが国際社会に発信され、国際世論を形成し、経済制裁の実施や国連総会決議などにつながった。中国の識者らは、情報戦や世論戦が今回のウクライナにおけるハイブリッド戦争の重要な領域との認識を示している[15]。国防大学の李海明は、「認知領域作戦は将来戦の主戦場であり、ウクライナ戦争は認知領域作戦の新たな特徴を出現させ、我々に多くの示唆を与えている」と指摘した。そのうえで今回のウクライナ戦争でみられた認知戦の特徴として、①指導者による政治的なナラティブの重要性、②ハイブリッド戦争の認知作戦の攻勢性、③平時における国際的プラットフォーム構築の重要性、④科学技

術が認知攻防に与える新規性の 4 点を指摘する[16]。

中国の識者の多くは、ウクライナ戦争にかかる国際世論形成において西側メディアが圧倒的に優位に進めたと評価する。彼らによれば、西側諸国のメディアは、ロシアがウクライナの領土を“侵略”したとのナラティブを展開し、ウクライナにおける人道危機やロシアによる虐殺事件を選択的に報道で取り上げ、ロシアによる侵略行為の不当性を幅広く国際世論に訴えることに成功した。とりわけ、グーグル、フェイスブックなどの米国のインターネット企業は SNS のアルゴリズムや運用規則などを変更してロシア政府系メディアの報道を排除したり、また、ユーチューブがスプートニクの欧州向けのアカウントを排除するなどした。この結果、ロシアによる宣伝工作は著しく制限され、西側の強力なメディア優位の前で能力を十分発揮することができなかったのである。

こうした評価をふまえて、中国の識者らは、西側諸国との国際世論戦において現状の圧倒的劣勢の現状に対して、いかに対応すべきかの検討を進めている。例えば、中国社会科学院の研究者は、「東昇西降（中国を含む東側がパワーを増大させ、西側がパワーを減少させることを意味する）」の長期的な国際関係の潮流は変わらないものの、現状の実力においては「西強東弱（西側が強く、東側が弱い）」という態勢は依然として変わっておらず、とくにネットワーク空間においては、これが顕著であると指摘する[17]。また、中国人民解放軍戦略支援部隊隷下の信息工程大学の研究者らも「世論や発言権をコントロールするという点で西強東弱という状況」を認めた上で、「（中国は）世論を攻撃・擁護する能力の強化を重視し、情報誘導の仕組みを改善し、インターネット上の新たなメディアに対する支援と投資を強化することによって、（西側の世論戦能力を）早く追い抜く」ことを提起する[18]。さらに、ある中国の識者は、新華社や人民日報、中央電視台などの中国の政府系メディアは、国際ニュース放送チャンネルの中国環球電視網（CGTN）をグローバル展開するなど国際的な影響力を増強させているが、これらに比べて中国系 SNS プラットフォームは海外の言論空間への影響力がなお弱いため、ティックトック（TikTok）のような米国市場に入り込む中国発の国際的な SNS プラットフォームの育成が急務と提起する[19]。

他方で、西側メディアの世論戦にあまり影響を受けなかった発展途上国・新興国、いわゆるグローバル・サウスの動きも中国で注目されている。中国社会科学院ロシア東欧中央アジア研究所の王晨星は、ウクライナ戦争の過程で国際政治構造が陣営化、集団化する傾向がみられるとした上で、こうした中でもグローバル・サウス諸国が対外政策の独立性を強化し、非同盟の立場を追求していることを指摘する[20]。王は、グローバル・サウス諸国は、ウクライナ戦争において、①中立的な立場を維持し、②西側の対ロ制裁をディカップリングや食糧危機を引き起こすとして批判し、③ウクライナ危機の政治的解決を主張するという特徴を指摘する[21]。さらに、ウクライナ戦争から汲み取る教訓として、中国は独立自主を維持し、短期的利益に基づいて米国に依存してはならず、非同盟原則のもとでグローバル・サウス国家間の相互連携を強化し、国際関係の民主化やグローバルな反覇権統一戦線の構築を進めることを提起している。

4.台湾有事に向けてどのように教訓を生かすか

これまで見てきたように、中国の人民解放軍関係者や研究者らは、ウクライナ戦争において、様々な教訓を引き出している。それでは、台湾有事に向けて、これらの教訓を生かすのであろうか。また、それは今後の軍建設や外交方針にいかなる影響があるのだろうか。

ウクライナ戦争において中国人民解放軍が教訓として引き出しているのは、現代の戦争が新たな安全保障領域や経済・金融・外交・科学技術領域を幅広く含むハイブリッドな要素を強める傾向にあることである。今回のウクライナ戦争が、ロシアによって仕掛けられたハイブリッド戦争というより、新たな技術や新たな領域が戦場に現れることによって戦争がハイブリッド化している、との見方が中国の識者らによって強調されている点は重要である。ハイブリッド戦争は、紛争の空間的・領域的な拡張により、域外国の介入の余地を生み、紛争の国際化を招く傾向にある。ウクライナ戦争を経て対ロシア批判という点において西側諸国の連帯は強固になり、その連帯感は対中姿勢にも反映されている。また、西側諸国によるハイブリッドな戦い方は、劣勢国ウクライナに軍事大国ロシアと戦える能力を付与しただけでなく、ロシアの総合国力を衰退させることにもつながっている。

こうした中国側のウクライナ戦争分析を踏まえると、中国が一方的に台湾に対して軍事行動を取る場合に仮に日米の直接的な軍事介入を抑止することに成功したとしても、西側諸国によるサイバー・認知を含む非物理的領域における軍事介入や補給活動・後方支援・経済制裁・外交工作にみられる間接的な関与を回避することは難しい、と中国側が評価すると推測される。また、「一つの中国」原則のような国家間の了解や抑止関係に縛られない民間企業や個人の紛争への関与は、中国側の算段を複雑にするであろう。前記したような中国におけるウクライナ戦争への評価を鑑みるに、軍事的観点から台湾武力侵攻を実施するハードルは、少なくとも短期的に高くなったと言えるだろう。他方で、当然ながら、中国は、台湾の解放をするための軍事統一シナリオを放棄するわけではないので、以上の困難を踏まえつつ、長期的に A2AD 能力・揚陸能力・市街地作戦能力、継戦能力を向上させるための努力を続けていくであろう。

また、中国人民解放軍がウクライナ戦争を観察する中で戦場で新興技術が軍事利用されていることで紛争の在り方が大きく変わりうることを再確認したことは明らかである。こうした意味では、習近平が示す「科学技術が現代戦争の核心的な戦闘力」という認識の下で「イノベーション型の人民軍隊を建設する」という軍建設の方針を継続するだろう[22]。習近平政権は近年、国際的な批判を避けるために軍民融合発展戦略を政府として掲げることを控えているものの、それに代えて「一体化国家戦略システム能力」という言葉を用いて、新興技術の軍事利用を促すために市民社会に対する動員体制を強化している[23]。

同様の観点から、習近平政権は将来戦と捉えている「智能化戦争」を戦うための軍隊建設

の方針を再確認しているであろう。ウクライナ戦争勃発後の 2022 年秋に開催された第 20 回党大会での演説において習近平は「機械化・情報化・智能化の融合発展を堅持する」としたうえで、「情報化・智能化戦争の特徴と規律を研究・掌握し、新たな軍事戦略指導を創新し、人民戦争の戦略戦術を発展させる」として、軍の智能化を進める方針を明確に示している[24]。ウクライナ戦争においては、各種無人機が活用されていることに中国側は注目していることを踏まえると、同演説で習近平が「無人智能化作戦能力を発展させる」と強調したことは示唆的である。こうした観点から、東シナ海や台湾海峡で近年活発化している無人機運用の実態や軍事的威圧の意図について注意を向ける必要があろう。

また、台湾への軍事侵攻のハードルが高い中で、中国にとっては、グレーゾーン作戦による漸進的な現状変更を継続することが重要となってくるであろう。2022 年のナンシー・ペロシ（Nancy Pelosi）下院議長の訪台以降、中国人民解放軍は中国軍機の中間線越えや威圧的な飛行を常態化させるなど漸進的な現状変更を進めている。こうした武力による威圧によって、台湾政府や市民に圧力を加え、半ば強制的に平和統一のテーブルに座らせる「強制的な平和統一路線」を目指している[25]。2024 年 1 月に実施された台湾総統選挙の結果が示すように、台湾に対する軍事的威圧は奏功していないものの、中国が軍事的威圧を弱める気配はみられない。

さらに、中国は、ウクライナ戦争の過程で、現状における「西強東弱」という状況を認識した一方で、中国が認識する「東昇西降」という長期的傾向を推進していくためにグローバル・サウスへの取り込みや宣伝戦を強化している。近年、中東やアフリカ諸国との高官交流の際には、相手国の高官に対して「一つの中国」原則への言及のみならず、軍事的圧力を念頭にして「主権擁護のための中国側が採る正当な措置への支持」というより踏み込んだ支持表明をさせるなど、外交的な働きかけを強めている[26]。また、アフリカ諸国で顕著にみられるように、中国政府系メディアの進出や現地メディア買収によるパブリック・ディプロマシーを展開し、先進諸国のみならず新興国も主な対象にして台湾有事を念頭に平時における世論戦を活発化させていくであろう[27]。地理的に離れたアフリカや中東地域においては、台湾海峡を含めた東アジア情勢に対する関心が低いため、同地域でバランスの取れた情報が提供されなければ、中国の立場に近い世論や政府見解が形成される可能性は否定できない。

[1] 趙小卓「従烏克蘭危機看戦争形態演変」『国家安全研究』2023 年 2 月 28 日、135-136 頁。
[2] 汪海江「依托一体化国家戦略体系和能力提昇戦区備戦打仗水平」『学習時報』2023 年 5 月 15 日。
[3] 徐舒悦・高飛「烏克蘭危機背景下“混合戦争”理論与実践評析」『平和与発展』2023 年第 4 期、79 頁。
[4] 例えば、顧煒「烏克蘭危機対地区競合及欧亜秩序的影響」『国際関係研究』2023 年第 2 期、25-42 頁など。
[5] 高雲「俄烏衝突一周年回望」『解放軍報』2023 年 2 月 23 日。
[6] 左希迎「非常規戦争与戦争形態的演変」『世界経済与政治』2020 年第 3 期、83-84 頁。
[7] 趙偉・李偉辰・劉光明「2022 年俄烏衝突中的網絡空間対抗情況総述」『網絡空間戦略論壇』2022 年 12 月、66 頁。
[8] 例えば、「威脅中国空間駅的星鏈衛星　背景不簡単」『新華網』2021 年 12 月 28 日。
[9] 「“星鏈”在俄烏衝突中的運用分析与思考啓示」『安全内参』2023 年 1 月 4 日。
[10] 趙小卓、前掲論文。
[11] 「警惕“星鏈”的野蛮拡張和軍事化応用」『解放軍報』2022 年 5 月 8 日。
[12] 「“星鏈”在俄烏衝突中的運用分析与思考啓示」『安全内参』2023 年 1 月 4 日。
[13] 王太軍、唐鰤綦、周超「“星鎖”在俄烏軍事衝突中的応用探研」『通信技術』（Vol,55 No.8）2022 年 8 月、1006-1013 頁。
[14] 同上。
[15] 徐舒悦・高飛「烏克蘭危機背景下“混合戦争”理論与実践評析」『平和与発展』2023 年第 4 期、86 頁。
[16] 李明海「認知域正成為未来智能化混合戦争主戦場」『環球時報』2022 年 3 月 17 日。
[17] 郎平「従俄烏衝突看網絡空間武器化傾向及其影響」『網絡空間戦略論壇』2022 年 6 月、66 頁。
[18] 曹衛東・宗留勇・曽相為「烏克蘭危機中網絡戦戦法分析」『信息安全与通信保密』2023 年 7 月号、27 頁。
[19] 武琼「烏克蘭危機中網絡空間対抗的影響及啓示」『俄羅斯東欧中亜研究』2023 年第 3 期、103 頁。
[20] 王晨星「烏克蘭危機与“全球南方”的政治崛起」『World Affairs』2023 年 12 月、18 頁。
[21] 王晨星、前掲論文、17 頁。
[22] 中国人民解放軍における科学技術振興政策については八塚正晃「『イノベーション型の人民軍隊』を目指す中国の政策と課題」『NIDS コメンタリー』2021 年 5 月 21 日。
[23] 「努力開創一体化国家戦略体系和能力建設新局面」『解放軍報』2023 年 3 月 9 日。
[24] 「習近平：高挙中国特色社会主義偉大旗幟為全面建設社会主義現代化国家而団結奮闘－在中国共産党第二十次全国代表大会上的報告」中華人民共和国中央人民政府、2022 年 10 月 25 日。
<https://www.gov.cn/xinwen/2022-10/25/content_5721685.htm>
[25] 「強制的平和統一」という習近平政権の対台湾政策は、松田康博氏や小笠原欣幸氏が提起している。
[26] 例えば、「王毅会見埃及外長舒克里」中国外交部、2022 年 9 月 25 日。
<https://www.fmprc.gov.cn/wjbzhd/202209/t20220925_10771192.shtml> この他、シリアのアサド大統領と 2023 年 9 月に合意した戦略パートナーシップ文書においては「中国政府が国家統一を実現するためにとる一切の努力を支持する」と言及している。「中華人民共和国和阿羅伯叙利亜共和国関於建立戦略伙伴関係的聯合声明（全文）」新華網、2023 年 9 月 22 日。 <http://www.news.cn/world/2023-09/22/c_1129878573.htm>
[27] Joshua Eisenman, “China’s Media Propaganda in Africa: A Strategic Assessment,” United States Institute of Peace, No. 516, March 2023.

第４章
サイバー空間の戦いとテック企業の関与

川口 貴久

はじめに

ロシアは 2022 年 2 月のウクライナ全面侵攻から今日に至るまで、ウクライナやその友好国に大規模かつ継続的なサイバー攻撃を実行してきた。特にキーウ攻防戦からドンバス・南部の戦いに移行するまで、ウクライナに対して破壊的・妨害的サイバー攻撃を試みた。しかし、これまでのところ、ロシアがサイバー空間を通じて戦争の趨勢に影響を与える効果を生み出していないという意味で、ウクライナはサイバー防衛に成功している。これは事前の予想や言説を大きく覆すものであった。長い間、当然視されてきたサイバー空間における「攻撃者優位」の前提は揺らいでいる。また、戦争を通じて変化するサイバー空間の攻防からは、戦時のサイバーセキュリティは「電撃戦」のみならず、「消耗戦」に備えるべきことを示唆する。

ウクライナのサイバー防衛「成功」[1]は多くの専門家の評価が同意するところだが、その要因については幅があり、強調される点は異なる。本章では、サイバー空間の戦いの「教訓」として、アマゾン、グーグル、スペース X、マイクロソフト、メタといった米国（や欧州の一部の）テック企業の前例のない支援と関与に焦点を当て、将来の紛争、特に中国が関与する紛争への示唆を検討する[2]。テック企業はウクライナのサイバー防衛に大きく貢献した。しかし、論点はこうした成功体験や「教訓」が将来の紛争にも適用可能かどうかである[3]。結論を先取りすれば、サイバー領域におけるウクライナ防衛を支えたテック企業の関与と貢献は、中国が関与する将来の紛争、台湾有事で再現できるかは極めて疑わしい。

本章はまず、ウクライナ戦争におけるサイバー領域の攻防を概括する。次に、サイバー防衛に関するウクライナの成功要因として、米欧のテック企業による関与と貢献に注目する。最後に、テック企業によるウクライナのサイバー防衛の台湾有事への適用可能性や再現性の観点での限界についてまとめる。

1.ウクライナ戦争とサイバー領域の戦い

（1）ロシアによるウクライナ全面侵攻とサイバー戦

ウクライナ戦争は 2023 年 11 月時点で、地上兵力と火力が勝敗を決する「20 世紀」型の戦争の様相を呈している。これまでのところ、ロシアによるサイバー攻撃が戦争の趨勢に影響を与えた事案は観察されていない。

サイバー領域におけるウクライナとロシアの攻防全てを記述することはできない。しかし、ウクライナ国家特殊通信・情報保護局（SSSCIP）幹部らの認識に基づけば、ロシアのサイバー戦は 3 つの局面に大別される。すなわち、①全面侵攻以前、②全面侵攻前後からキーウ攻防戦、ロシアの転戦（2022 年 2 月から 4 月）、③ドンバスおよび南部の戦い以降（同年 4 月以降から現在）である[4]。

「全面侵攻以前」のサイバー戦がいつ始まったかを定義することは難しい。2021 年以前からウクライナは常にロシアによるサイバー攻撃の標的だったからだ。しかし、ウクライナ SSSCIP のビクトル・ゾラ（Viktor Zhora）副局長は「ロシアのサイバー攻撃が始まったのは 1 月 14 日」「2 月 24 日より前から戦いは始まっていた」という[5]。1 月 14 日の攻撃とは約 200 のウクライナ政府や企業のウェブサイトが攻撃を受け、「最悪を覚悟しろ」という脅迫メッセージに改竄された事案である。こうした攻撃の狙いについて、ユーリ・シチホリ（Yurii Shchyhol）SSSCIP 局長は「多くのウクライナ国民をパニックに陥らせ、ウクライナが攻撃に対処できない弱小国家であることを世界に示すこと」「攻撃の結果は心理戦に近い」と指摘する[6]。

「全面侵攻前後からキーウ攻防戦」に至る期間では、ロシアによる多くの破壊的・妨害的サイバー攻撃が観察された。24 日の全面侵攻の約 1 時間前、ウクライナ政府・軍・治安機関が契約する米国ビアサット（ViaSat）社所有の KA-SAT 衛星ネットワークで障害が発生した。後に米英政府はこの攻撃をロシア連邦軍参謀本部情報総局（GRU）が関与したと判断した。障害を引き起こしたのは、地上のルータに対する DDoS 攻撃と「AcidRain」と呼ばれるワイパー型（データ消去型）マルウェアによるものとみられている。ロシアは AcidRain 以外にも、前例のない規模でワイパーを開発・展開した。全面侵攻以前から 4 月末まで、標的とする OS、破壊対象の領域、用いられたプログラミング言語等が異なる 9 種類のワイパーが投入された[7]。これはロシアが相当なリソース（資金、要員、時間、技術的資産等）を対ウクライナ戦初期に投入したことを示唆する。

「ドンバスおよび南部の戦い以降」も破壊的サイバー攻撃が指摘されているが、それは 2022 年春とは様相が異なる。前述のゾラ副局長は 2022 年 3 月末から 4 月初旬は「多くの非常に洗練されたサイバー攻撃」を受けたが、同年 10 月時点でロシアのサイバー活動に「特定の戦略」は見いだせず、むしろ「場当たり的な振る舞い」だという。つまり、攻撃はとに

かく脆弱性を探し続け、それを悪用し、永続化した上で、それをどう使うのかを決める。ロシア側に戦略が欠如しているため、ウクライナ側も脆弱性を修正し続け、インシデントに対処するという基本的なものだという[8]。

ただし、これは2022年春以降のロシアのサイバー戦に変化がない、という意味ではない。むしろロシアによるサイバー活動の狙い、重点的な標的となる産業、戦術・技術・手順等は常に変化し続けている[9]。「狙い」という点では、ウクライナを標的にするロシアのハッカーは、破壊的・妨害的な攻撃から方針を転換し、ロシア軍が「戦場で有利になる」データや情報の収集（諜報型のサイバー攻撃）にますます重点を置くようになった[10]。長期化する地上の戦争によって、サイバー戦も「消耗戦」というべき様相を呈している。

（2）サイバー空間におけるウクライナの優位性をめぐる議論

ロシアはその継続的なサイバー作戦にも関わらず、大きな効果を生み出していない。これは多くの専門家の見立てと一致するが、その要因については幅があり、強調される点は異なる。全面侵攻直後、ロシアはウクライナに対して破壊的サイバー攻撃を「行っていない」「選択しなかった」「抑制している」との見方もあった。しかし、現時点ではこうした見立ては概ね否定され、ウクライナはどのようにして成果をあげたのか、事前の予測とは何が異なっていたのか、という観点が多い[11]。具体的には、破壊的サイバー攻撃の生来的な制約と限界、ロシア側の（必ずしもサイバーに限定されない）計画・組織・ドクトリン、ロシアによるサイバー空間でのエスカレーション管理等、様々な仮説が指摘されている。

しかし、多くの分析で指摘されているのはウクライナ自身によるサイバー防衛の改善である。つまり、2014年のクリミア併合と東部紛争以降のサイバー防衛分野への投資であり、2022年2月の開戦前後以降の脅威への適応である。加えて注目すべきは、米欧政府やテック企業がウクライナ防衛の姿勢を旗幟鮮明とし、大規模かつ継続的な支援を行ってきたことである。例えば、カーネギー国際平和基金のジョン・ベイトマン（Jon Bateman）は、ロシアによるサイバー活動の効果が低調である要因として25の仮説を整理し、米欧政府や民間のテック企業によるウクライナ支援を大きな要素として指摘している[12]。米国サイバー軍（USCYBERCOM）をはじめとする米英政府等の支援実態はごく一部を除いて秘密のベールに包まれているが、米欧の民間企業の支援は実態が明らかになっている。

2.ウクライナ戦争とテック企業の関与

（1）テック企業の関与

全面侵攻前から今日まで、ウクライナ政府と米欧テック企業の協力関係は確認されている。ただし、米欧テック企業の支援は自明だったわけではない。特に全面侵攻直後から、サ

イバー空間（および認知領域）における優勢確保のため、ウクライナ政府は国内外のテック企業に協力を要請した。その数は侵攻翌週の 3 月 5 日時点で 70 社超、3 月 14 日時点には 200 社を超えたという[13]。ボロディミル・ゼレンスキー（Volodymyr Zelenskyy）大統領やミハイロ・フェドロフ（Mykhailo Fedorov）副首相兼デジタル転換相自ら協力を要請することもあった。

ウクライナ戦争に関与したテック企業は幅広い。ここでいう「テック企業」とは、情報通信技術を基に製品、サービス、インフラ等を提供する企業全般を指す。これは、異なるステークホルダーに何か（ビジネス、交流等）を行う「場」を提供する「デジタルプラットフォーム（DPF）企業」やコメント、動画等のユーザー生成コンテンツ（User Generated Contents: UGC）の生成・交換・受発信・保存等を可能にする「ソーシャルメディア企業」を包含するものである。ウクライナ戦争に関与したテック企業は、IT ベンダ（ソフト、ハード）、セキュリティサービス、インターネットサービスプロバイダ（ISP）、衛星画像や衛星通信等の宇宙サービスと多岐に渡る。

また戦争に対するテック企業の姿勢という点では、徹底的なウクライナ支援とロシア対抗を明言するテックもあれば、インターネットの本来の設計思想に基づき中立を維持するテック企業もみられた。概していえば、セキュリティやソーシャルメディア等のコンテンツに近い階層では前者、インターネットの基盤に近い階層では後者を重視しているように見受けられる[14]。こうしたテック企業の関与の形態は、①ウクライナへの人道支援、②ウクライナの防衛、③ロシアの弱体化に整理できる。「人道支援」とはウクライナ人ユーザーのセキュリティやプライバシー保護の強化、有益な情報や信頼できる情報源の集約や優先的表示（空襲警報アプリやシェルター等の安全情報、募金支援先等）等であり、「弱体化」とはロシア向け事業の縮小・中断・撤退（ISP 世界大手によるロシア向けのインターネット接続サービスの停止等）等である。本章ではサイバー空間の「ウクライナの防衛」に焦点を当てて具体例を紹介する。

（2）代表的なテック企業の関与とウクライナのサイバー防衛

数多くのテック企業は様々な形態でサイバー空間の「ウクライナ防衛」に貢献した。

衛星通信サービスの提供（スペース X）

2022 年 2 月、ロシアによる物理的攻撃によってウクライナ地上の通信インフラが破壊され、サイバー攻撃によってウクライナの大手 ISP や（前述の）ViaSat 社の衛星通信ネットワークに障害が発生した。こうした被害が生じた通信インフラを代替したのが、低軌道衛星コンステレーション通信サービス「スターリンク」であった。フェドロフ副首相がツイッター（現 X）上でスペース X 社のイーロン・マスク（Elon Musk）に、ウクライナへのスターリンク提供を要請し、マスクが即時に応えた。高速かつ低遅延の通信サービスを提供可能なスターリンクはウクライナ政府・軍の通信のみならず、ドローンをはじめとする攻撃関連の

指揮命令・通信にも用いられ、ウクライナ政府や市民による国内外のコミュニケーション・情報戦にも貢献している[15]。スターリンクはウクライナの防衛戦争にとって不可欠であり、テック企業のウクライナ支援の象徴ともいえる。しかし、それゆえ、スターリンクは別の問題を惹起している（後述）。

重要データの防護とクラウド化　（AWS、グーグル、マイクロソフト等）

ウクライナ戦争では、重要データのクラウド化と友好国への分散が行われた。アマゾンウェブサービス(AWS)、グーグル、マイクロソフト、ヴイエムウェア（Vmware）はウクライナ政府が保有する重要データのクラウド化とバックアップを支援し、これはウクライナ人に対するデータ移行やクラウド関連のトレーニング提供を含む。全面侵攻 1 週間前の 2 月 17 日、ウクライナ議会は、政府のデータを既存のオンプレミスサーバからクラウドに移行することを許可するため、データ保護法を改正した。結果、政府の重要データをウクライナ国外、欧州の複数のデータセンターに分散退避させることが可能となった[16]。事実、侵攻後、ウクライナ国内のオンプレミスのデータの一部（自動車保険に関するデータ）がミサイル攻撃によって破壊されたが、バックアップにより迅速に復旧できたという。

サイバー攻撃や脅威の検知・対処　（マイクロソフト、ESET、クラウドフレア他多数）

マイクロソフトやスロバキアのウイルス対策ソフト企業 ESET 等はセキュリティ製品・サービスを通じてウクライナ向けのサイバー攻撃を検知・対処し、収集されたデータ・脅威情報を将来のサイバー防衛に活用した。明らかになっている顕著な成果の一つは、ESET がウクライナのナショナルサート（CERT-UA）と協力し、電力インフラへの破壊的サイバー攻撃を防いだことだ。この他にも、グーグル、クラウドフレア、シスコ、ビットディフェンダー（BitDefender）、レコーデッドフューチャー、SAP 等の多様な業態のテック企業がウクライナ政府関係機関や企業に、サービスやライセンスの提供・更新を無償で行った。

こうした大手テック企業のデータ収集は、多くの主権国家を凌駕する。米国に次ぐサイバー能力を有するとみられる英国でサイバー戦を担う戦略軍副司令官によれば、「[英戦略軍が] 防衛の一環で収集しているサイバー脅威データの量に大きな自信を持っているが、マイクロソフトが日々集めているものに比べれば微々たるもの」と述べるほどだ[17]。

情報戦への対処　（グーグル、ツイッター、メタ等）

グーグル、ツイッター、メタ等のデジタルプラットフォームは様々な形でロシアの情報戦に対処してきた。テック各社の対応は強制力の度合いから、(1) 政府規制への対応、(2)執行強化要請への対応、(3) 自主的取組みの三つに大別できる。第一に全面侵攻直後の 3 月 2 日、欧州連合はロシア政府系メディア「RT」および「スプートニク」らの衛星放送、オンラインプラットフォーム、アプリ等の EU 域内での活動を禁止した。第二に、ベラ・ヨウロバー（Vera Jourova）欧州委員会副委員長（価値観・透明性担当）は、DPF に対して、外国

の影響力行使に関する執行強化を要請した。欧州委員会は、DPF 各社に「ロシアの在外公館アカウントや政府機関アカウントの広範なネットワークがロシア政府に属することに鑑みて利用規約を厳しく適用し、法律やサービス規約に反するコンテンツに直ちに対処[18]」するように求めた。最後に、DPF 各社は、事業者としての自主的対応（自主規制）を講じた。ロシア政府系メディアであることのラベリング、こうしたメディアの収益化の制限、レコメンドシステムのアルゴリズム変更といった措置である[19]。

3.台湾有事にテック企業の関与を期待できるか

ウクライナ戦争におけるテック企業のサイバー防衛への貢献を以って、「サイバー国連」や「テック NATO」を設立すべきとの声すらあがる。つまり、民間企業を含めたサイバー空間の集団安全保障または集団防衛である。しかし、ウクライナ戦争でみられたテック企業の関与による「成功」が将来に適用可能かは疑わしい。特に、台湾有事を念頭においた場合、テック企業の関与や貢献は大きな不確実性や限界がある。

（1）テック企業の意思決定の不確実さとガバナンス

ウクライナ戦争は、ロシアによる侵略行為が既存の国際秩序・規範に反することが明らかであり、中立よりも積極的なウクライナ支援・ロシア対抗を選択したテック企業は少なくなかった。しかし、対立構造や価値判断が明確なウクライナ戦争であっても、テック企業は困難なジレンマに直面し、その意思決定が戦争の趨勢に影響を与えるケースさえあった。

その典型はスペース X である。同社の最高経営責任者であり、筆頭株主であるマスクは 2022 年 10 月、ロシアによる現状変更を追認するような独自のウクライナ戦争「和平案」を提示し、ゼレンスキー大統領らの反発を招いた。また、マスクは経済的コストを理由に、将来のスターリンクの提供を見直す考えも示唆した。より直接的に、マスクがウクライナ軍の作戦に影響を与えることもあった。同氏の公式評伝によれば、ウクライナ軍がクリミア半島のセバストポリでスターリンクを使用したいという緊急要請をマスク自らの判断で拒否した。その直前、ロシア大使から戦争のエスカレーション（クリミア半島への攻撃）に関する懸念が示されたことをふまえての判断だという[20]。スペース X 社はウクライナ軍を含むウクライナの防衛作戦にスターリンクが使用されることは問題ないとしつつも、ウクライナ領土内であってもロシア軍攻撃にスターリンクが活用されることに難色を示し、そうした利用を制限した[21]。

確かにスペース X 社はその業務執行、出資にマスクが決定的な影響力を持つというコーポレート・ガバナンスおよび内部統制上の問題を抱える。しかし、これは程度の差こそあれ、同社に限ったことではない。2021 年 1 月 6 日の米国議事堂襲撃事件に関する対応をはじめ、DPF の意思決定の妥当性や透明性が問題となってきた。ウクライナ戦争開戦直後、メタ社

内ではフェイスブックやインスタグラムといった同社のプラットフォーム上で、従来の利用規約を見直して、「ロシアの独裁者に死を」といった投稿を認めるかどうかで議論があった。「見直し」派によれば、こうした投稿を規制することが、ウクライナ市民の団結と侵略への抵抗を阻害するという。侵攻直後、利用規約は一時的に見直されたが、その後、条件を絞る形で再修正された[22]。

このような状況をふまえると、中国共産党にとって「国内問題」である台湾有事について、テック企業はより複雑なジレンマと意思決定に直面することは間違いない。特に中国に市場、サプライチェーン、タレント（人財）を依存するテック企業はウクライナ戦争とは異なる深刻な経営課題となるだろう。

（2）異なる通信インフラ環境

ウクライナと台湾は前提となる通信インフラが大きく異なるため、テック企業がウクライナ戦争と同様の支援が可能かは疑わしい。

ウクライナの国際的なインターネット通信の大部分は（ロシアが実効支配するクリミア半島東端とロシアを結ぶ、短い海底ケーブル 2 本を除けば）国境を接する国々との地上の通信網に依存してきた。地上インフラが破壊され、ウクライナ国内の通信には障害が発生したとはいえ、国際的トラフィックが途絶えたわけではなかった。

他方、台湾は日本と同様、国際的なインターネット通信の 99%以上を海底ケーブルに依存する。2023 年 2 月 2 日および 8 日、台湾本島と馬祖列島を結ぶ海底ケーブル 2 本が、中国籍船舶によって切断される「事故」が発生した。全世界で年間約 100 件の海底ケーブル障害が発生しているものの、近い海域で短期間に発生した「事故」については様々な疑念を生じさせている。ただし、有事で懸念されているのは海底ケーブルの切断よりも、これらが複数陸揚げされる拠点（やその近傍）への物理的攻撃であり、海底ケーブルの陸揚げ拠点は新北市や東部の宜蘭県頭城鎮に集中している。

加えて、中国政府とその影響下にある通信企業が近隣および世界のインターネットトラフィックを再ルーティングする能力を示唆していることも大きな懸念点だ[23]。

ウクライナ戦争や 2 件の海底ケーブル遮断事故を目の当たりにした蔡英文政権は非静止軌道の衛星通信インフラの拡充に取り組んでいる。台湾政府独自の低軌道通信衛星の開発、地上の受発信設備の設置、それぞれ英国とルクセンブルクに拠点をおくユーテルサットワンウェブ（Eutelsat OneWeb）および SES との連携を強化している。唐鳳（オードリー・タン）デジタル発展部部長によれば、複数の衛星通信プロバイダとの連携は単に冗長性確保のためだけではなく、有事を念頭に「異なる国々に属する様々な衛星システムを一度にジャミングや妨害することは非常に困難[24]」だからだ、という。

（3）中国のサイバー戦に関する蓄積の少なさ

ウクライナのサイバー防衛に貢献したテック企業は、ロシアのサイバー攻撃と対処に関

する情報・ノウハウを長年に渡って蓄積し、これらを活用した。しかし、これら企業の中国関連の蓄積はロシア程ではないだろう[25]。例えば、中国はロシアほど妨害的・破壊的サイバー攻撃を対外的に見せつけていない。それは中国に破壊的サイバー能力がないということではなく、2020 年 10 月のインド・ムンバイ停電や 2023 年 5 月に明らかになったグアム他の重要インフラへの侵入能力が示している通り、中国は破壊的サイバー攻撃能力やそのために必要な偵察・事前配置能力を有していることはほぼ確実だ。2023 年の米国情報コミュニティ『年次脅威評価』や米国防総省の中国関連年次報告書も、中国が重要インフラに対する破壊的・妨害的能力を高度化させていると判断する。有事という点では、2015-16 年の中国人民解放軍の大規模再編以降、サイバー能力を集中化させている「戦略支援部隊」と引き続き破壊的能力を有する「戦区司令部」に紐づくサイバー攻撃グループに注視する必要がある。中国のサイバー活動や情報戦に関する戦術・技術・手順に関する知見・インテリジェンスを持つテック企業の関与が不可欠だ。

おわりに

ロシアは、ウクライナ全面侵攻開始の前後から今日まで、ウクライナに継続的なサイバー攻撃を展開してきた。しかし、ロシアがサイバー攻撃を通じて戦略的・戦術的効果を創出していないという意味で、ウクライナはサイバー防衛に成功している。その要因として、ウクライナ自身によるサイバー防衛の改善をはじめとして様々な解釈や仮説が考えられるものの、本稿では米欧のテック企業による関与に焦点を当てた。具体的には、低軌道衛星コンステレーションを通じた通信インフラの提供、重要なデータのクラウド化と友好国への分散、戦時における政府や重要インフラ企業に対するサイバーセキュリティサービスや脅威インテリジェンスの提供、オンラインにおける影響工作への対処という点で、テック企業はウクライナのサイバー防衛に大きく貢献した。

現在進行形のサイバー戦を扱っているため、アクセス可能な資料や情報は限られ、かつウクライナ側やテック企業が公開したものに偏重する等の課題は存在するものの、テック企業の関与はウクライナのサイバー防衛の重要な教訓であろう。同時に、この教訓は台湾有事等の東アジアの潜在的紛争に適用できるかは疑わしい。なぜなら、ウクライナ戦争とは異なる紛争の構図・対立関係、通信・情報環境、敵対者を想定しなければならないからだ。

サイバー空間の基盤とサイバーセキュリティの大部分をテック企業に依存している以上、テック企業の協力と支援を引き出すことはサイバー防衛に不可欠だ。しかし現状では、将来の紛争におけるテック企業の関与とサイバー防衛の成功は楽観視できるものではない。

[1] 本章は紙幅の関係で、情報戦や認知領域の戦いは割愛している。これについては、川口貴久「ウクライナ戦争と『ナラティブ優勢』をめぐる戦い」シノドス、2022 年 5 月 21 日；「ウクライナ米欧 VS ロシア 認知空間での闘いの内幕」Wedge Online、2022 年 4 月 29 日を参照。

[2] テック企業に注目した分析として、Brandon Bohrn, "Four Tech Lessons Learned from the Ongoing War in Ukraine," New Perspectives on Global European Dynamics, March 22, 2023; Christine H. Fox and Emelia S. Probasco, "Big Tech Goes to War: To Help Ukraine, Washington and Silicon Valley Must Work Together," *Foreign Affairs*, October 19, 2022.

[3] 台湾有事への適用を検証した数少ない分析として、Dan Black, "Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences," Research Paper, International Institute for Strategic Studies (IISS), March 28, 2023 の"Chapter Five: Lessons for a Taiwan Contingency" (pp.19-21)。 必ずしもサイバー戦に限定されるものではないが、Franz-Stefan Gady, "6 Wrong Lessons for Taiwan From the War in Ukraine: A potential Asian war would look very different," *Foreign Policy*, November 2, 2022.

[4] Google の 脅威分析グループ（TAG）、マンディアント（Mandiant）等の分析に基づく報告では、ロシアの 2022 年のサイバー攻撃は 5 つのフェーズに分類され、上記でいう「ドンバスおよび南部の戦い」を 3 つに細分化する。Shane Huntley, "Fog of war: how the Ukraine conflict transformed the cyber threat landscape," Google Blog, February 16, 2023.

[5] 「ロシアのサイバー攻撃、始まりは 1 月 14 日ハイブリッド戦の舞台裏」『朝日新聞』2022 年 7 月 29 日。

[6] 「ロシアからのハッキングに対抗するウクライナ、その"サイバー戦争"の指揮官の勝算」Wired、2022 年 9 月 22 日。

[7] Insikt Group, "Overview of the 9 Distinct Data Wipers Used in the Ukraine War," *Recorded Future*, May 12, 2022.

[8] Peggy Kelly and Bruce Sussman, "Ukraine Cybersecurity Leader Shares Defense Insights from Cyber and Physical Front Lines," BlackBerry Blog, October 27, 2022.

[9] 例えば、重点的な標的産業は、メディア・通信業界、エネルギー業界、法執行機関（ロシアの戦争犯罪に関連する情報収集と攻撃の標的）といった推移がみられる。"Russia's Cyber Tactics: Lessons Learned in 2022," SSSCIP, March 8, 2023; "Russia's Cyber Tactics H1'2023," SSSCIP, September 2023.

[10] Christian Vasquez, "Ukrainian official: Russian hackers change tactics from disruptive attacks," *Cyber Scoop*, August 9, 2023.

[11] James Andrew Lewis, "Cyber War and Ukraine," Center for Strategic and International Studies (CSIS); June 16, 2022; P.W. Singer, "One Year In: What Are The Lessons from Ukraine For The Future Of War?" *Defense One*, February 22, 2023; Kenneth Geers, eds, *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO Cooperative Cyber Defence Centre of Excellence: CCDCOE, 2023; Grace B. Mueller, et.al, "Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures," Center for Strategic and International Studies (CSIS), July 13, 2023; 大澤淳「新領域における戦い方の将来像：ロシア・ウクライナ戦争から見るハイブリッド戦争の新局面」、高橋杉雄 編著『ウクライナ戦争はなぜ終わらないのか：デジタル時代の総力戦』文藝春秋、2023 年、等。

[12] ベイトマンの整理はロシア関連の記述で主観的な形容詞や副詞が散見され、各仮説の記述レベル・粒度が異なるものの、現時点で最も包括的な分析であろう。 Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Cyber Conflict in the Russia-Ukraine War paper series, Carnegie Endowment for International Peace, December 16, 2022.

[13] 「ウクライナ、デジタル戦協力要請 200 社に　課題も浮上」『日本経済新聞』2022 年 3 月 17 日。

[14] 川口貴久「戦争とテック企業：ロシアによるウクライナ全面侵攻とテック企業の対応」スマートニュー

スメディア研究所、2023 年 2 月 14 日。

[15] 川口貴久「ウクライナ戦争で見えた『スターリンク』の凄さとリスク」Wedge Online、2022 年 10 月 19 日。

[16]「ウクライナの防衛: サイバー戦争の初期の教訓」日本語版、マイクロソフト、2022 年 6 月 22 日、5 頁。

[17] Alexander Martin, British Army general says UK now conducting 'hunt forward' operations, *The Record*, September 25, 2023.

[18] 「ロシアの偽情報対策を求められる米 IT 大手」『日本経済新聞』2022 年 3 月 23 日。

[19] 一定規模以上のプラットフォームに対して、違法・有害情報の対処やユーザーの権利保護を要求する欧州デジタルサービス法（DSA）では、戦時を含めた危機下での協調をテック企業各社に要求する。DSA に基づき、欧州委員会コミュニケーションネットワーク・コンテンツ・技術総局はウクライナ戦争下での DPF 各社のロシアへの情報戦対応状況を評価している。European Commission, Directorate-General for Communications Networks, Content and Technology, *Digital Services Act: Application of the risk management framework to Russian disinformation campaigns*, Publications Office of the European Union, 2023, pp.44, 46-47, 49, 65-72.

[20] ウォルター・アイザックソン（井口耕二訳）『イーロン・マスク』下巻、文藝春秋、2023 年、164-174 頁。

[21] Jeff Foust, "Shotwell: Ukraine 'Weaponized' Starlink in War against Russia," *Space News*, February 8, 2023.

[22] 「ＦＢ、ロシア兵への暴力呼び掛けを一時容認　ウクライナ関連のみ」ロイター、2022 年 3 月 11 日; 「米メタがウクライナ向け規約変更、国家元首の死求める投稿禁じる」ロイター、2022 年 3 月 11 日; Nick Clegg(@nickclegg)によるツイッター投稿、2022 年 3 月 12 日。
< https://twitter.com/nickclegg/status/1502349805221126144 >

[23] Black, Op. Cit.

[24] Kelvin Chen, "Taiwan ramps up efforts to finish backup satellite network," *Taiwan News*, Sep 23, 2023.

[25] Black, Op. Cit.; Gady, Op. Cit.

第５章
サイバーセキュリティと政治体制

山本 達也

1.「民主主義の後退」とインターネット環境の変化

本章のテーマは、政治体制とサイバーセキュリティに関する現状と課題についての論点を提示することにある。とりわけ、「インターネットの自由」をめぐる国際的な環境変化についてデータを使いながら近年の推移を分析し、サイバーセキュリティと民主主義との関係性について検討を行っていく。

近年、先進民主主義国の民主主義度が下落傾向にあるという「民主主義の後退（democratic recession）」現象が、全世界的に確認されている[1]。民主主義の後退というよりは、より積極的な形で「権威主義体制の復活」とも呼べる状況だとの指摘もある[2]。新型コロナウイルスの感染症に直面した際には、民主主義体制と権威主義体制のどちらの方がこの種の危機に効果的に対応できるのかという議論にも注目が集まった。これら 2 つの政治体制間の緊張と競争は、この先数十年にわたって繰り広げられる可能性が高い。

民主主義の後退と同様に、「インターネットの自由の後退」とでも呼べる状況も進行している。この現象は、非民主主義国に限ったものではない。かつて、「インターネットの自由」を促進させようとしていた先進民主主義国においてもスタンスの変化がみられるようになっている。背景には、サイバーセキュリティへの要請の高まりも関係している。

2013 年に起きた「スノーデン事件」において、エドワード・スノーデン（Edward Snowden）は、米国の国家安全保障局（NSA）の運用するインターネット監視プログラムについての機密情報を内部告発の形で暴露した。この暴露は、「安全かプライバシーか」という根本的な問いを社会に投げかけることになった。当初は、国家安全保障と個人のプライバシー保護という二律背反の状況をめぐって、後者が軽視されているのではないかという議論が行われていたが、次第に勢いを失っていったように感じられる。なぜなら、政策論的に突き詰めていくと、現代の国際環境の中で国家の果たすべき役割を果たそうとするならば、サイバーセ

キュリティを強化せざるを得ないのが現実だからである。

サイバーセキュリティの強化は、民主主義国における制度的な根幹とも言える選挙を外国勢力から守る上でも重要な政策課題となっている。この点、2016 年に行われた 2 つの投票は、象徴的な事例として注目に値する。1 つは、英国の EU からの離脱を問う国民投票で、もう 1 つは、ドナルド・トランプ（Donald Trump）前大統領が当選を果たした米国大統領選挙である。いずれのケースでも、ソーシャルメディアを介した投票行動の操作が指摘されている[3]。

ところが、2020 年に行われた米国大統領選挙においては、2016 年ほどインターネットを介した投票行動の操作が問題となっていない。その理由は、2016 年の経験を経て、サイバーセキュリティを担当する「サイバー軍」がうまく機能したからだと考えられている[4]。民主主義的な価値であるプライバシーの保護をある程度犠牲にしなければ、民主主義的な社会の制度的基盤である選挙を外国勢力から守ることが難しい時代になっているのである。

こうした背景を踏まえ、本章では、政治体制という視点からインターネットの自由をめぐる変化とサイバーセキュリティとの関係について論じていく。以下、第 2 節では、インターネットの自由をめぐる近年の変化についてデータを交えながらその推移を提示する。第 3 節では、先端技術をめぐるイノベーションと政治体制との関係性について検討する。第 4 節では、近年注目される人工知能（AI）がこの問題にどのように関係してくるのかについて議論する。最後の第 5 節では、これらの議論を総合し、昨今のウクライナ情勢等も視野に入れた上で民主主義国への教訓について考えていきたい。

2.「インターネットの自由の後退」が進行する世界

国際人権 NGO のフリーダムハウス（Freedom House）は、2011 年から「インターネットの自由（Freedom on the Net）」に関する年次報告書を継続的に刊行し、対象国のインターネットの自由度スコアを発表している。最新の 2023 年版では、70 ヵ国が調査対象となっており、全世界のインターネットユーザーの 88%をカバーしている[5]。

この調査では、各対象国について「A：アクセスへの障害（obstacles to access）」、「B：コンテンツ制限（limits to content）」、「C：ユーザーの権利の侵害（violations of user rights）」という 3 つのカテゴリにおいて 21 の独立した指標を用いて点数化をし、インターネットの自由度スコアを算出している。スコアは、0 から 100 の範囲で示され、スコアが 100 から 70 の国を「自由（free）」、69 から 40 の国を「部分的に自由（partly free）」、39 から 0 の国を「不自由（not free）」として分類している。

全世界の平均値を計算すると、2013 年が 54.63 で最も高く、以来 2023 年に向けて低下傾向にある。2023 年のスコアと、2013 年のスコアを比べたときに、最も下落幅の大きい国はミャンマーであり、以下、ロシア、トルコ、ベネズエラ、ルワンダ、ウガンダ、フィリピ

ン、キルギスタン、リビア、ウクライナと続く。

V-Dem 研究所（V-Dem Institute）が公開している民主主義に関するデータセットにおける政治体制等の要素を考慮に入れた地域区分を適用して、各地域におけるインターネットの自由度スコアの推移を分析してみても、すべての地域でインターネットの自由度スコアは低下傾向にある（図 5-1 参照）[6]。同じ地域区分で、V-Dem 研究所による自由民主主義度のスコア（0 から 1 の値をとり、1 に近いほど自由民主主義度が高いことを示す指標）の推移を分析すると、サハラ以南アフリカおよび東欧・中央アジアではスコアが増加傾向にある。インターネットの自由度が、どの地域も下落傾向にあることと対照的である。

図 5-2 は、フリーダムハウスが示す「A：アクセスへの障害」、「B：コンテンツ制限」、「C：ユーザーの権利の侵害」という 3 つのカテゴリのうち、どのカテゴリがインターネットの自由度のスコアを引き下げているのかを調べるために、「自由」、「部分的に自由」、「不自由」の区分ごとに、各スコアの推移を示したものである。このグラフを見ると、どの評価区分においても「アクセスへの障害」について改善がみられる。逆に、どの評価区分でも一貫して下落傾向にあるのが、「ユーザーの権利の侵害」カテゴリである。また、不自由と評価される国では、「コンテンツ制限」カテゴリで大幅にスコアを下げていることが読み取れる。

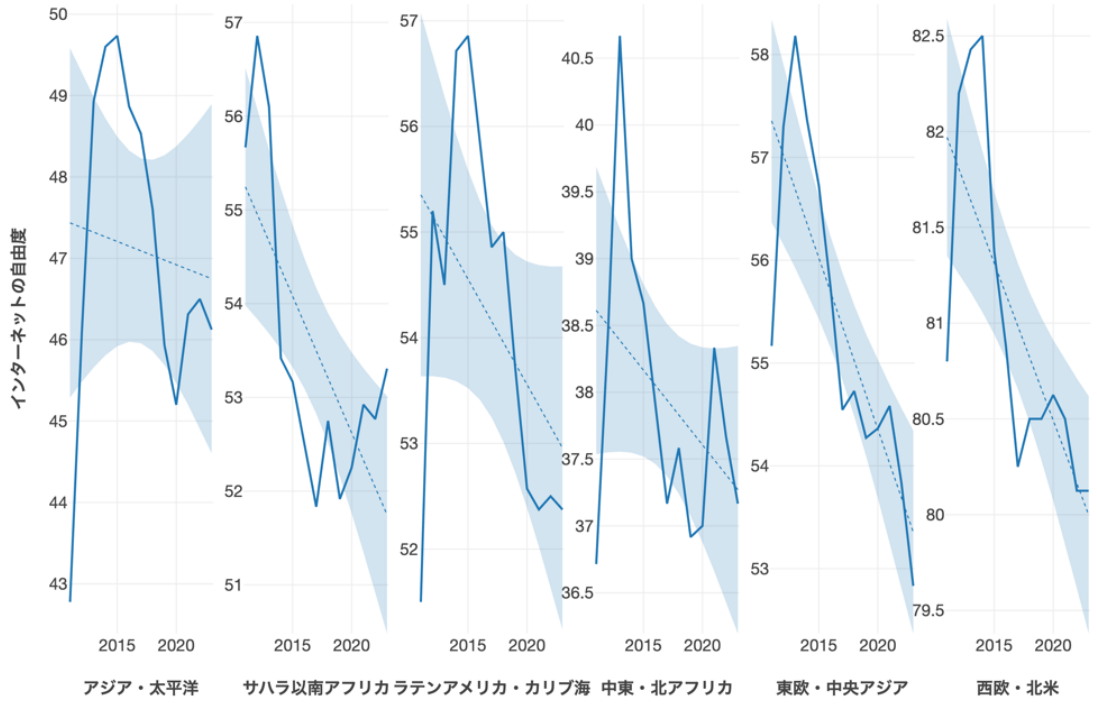

図 5-1：地域区分ごとにみたインターネットの自由度スコアの推移

（出典）筆者作成。データは、フリーダムハウスによる Freedom on the Net のスコアを使用。地域区分は V-Dem Dataset（v.13）の politico-geographic 6-category（e_regionalpol_6C）を適用。なお、地域ごとの傾向の詳細を確認するため Y 軸は同期させていない。破線は回帰直線、網掛けは 95%信頼区間を示している。

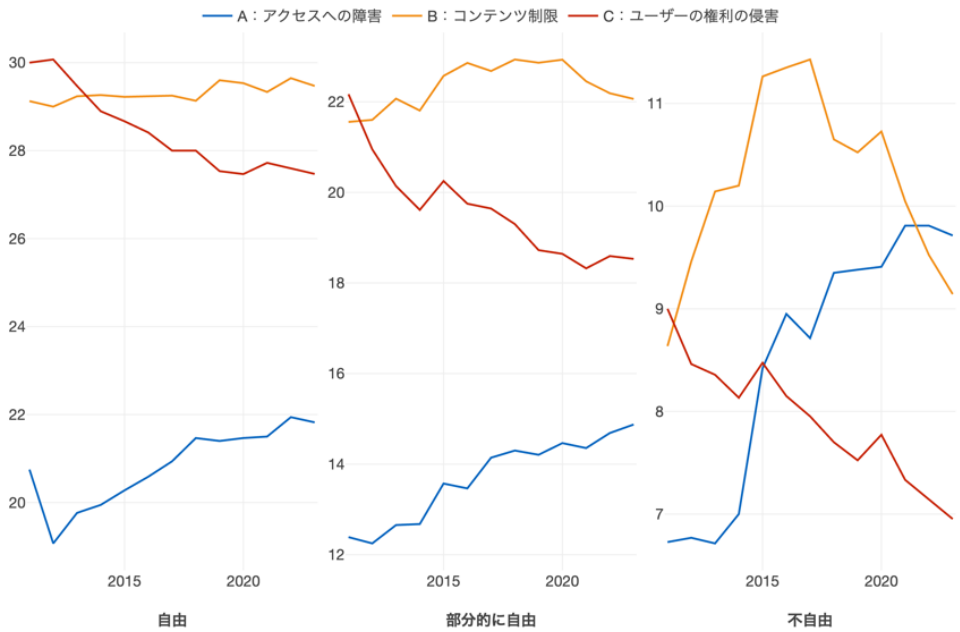

図 5-2：インターネットの自由度を構成する 3 つのカテゴリのスコア推移

（出典）筆者作成。データは、フリーダムハウスによる Freedom on the Net のスコアを使用。なお、評価区分ごとの傾向の詳細を確認するため Y 軸は同期させていない。

自由と評価されるような国を含めて、スコアを下げている「ユーザーの権利の侵害」カテゴリであるが、ここに含まれるのがまさに「表現の自由」や「プライバシーの保護」と関係が深い項目である。自由と評価される国では、このカテゴリ以外は横ばいか改善がみられる。ここにサイバーセキュリティへの要請が高まる中での、民主主義国の苦悩が表れていると言えるだろう。

3. 先端技術をめぐる体制間競争とイノベーション

民主主義体制と権威主義体制との競争は、先端技術分野のイノベーションでも行われるようになっている。特にこの分野での中国の存在感は増しつつあり、かつてのように経済的繁栄や先端技術の恩恵を得る上で民主主義体制が有利だというコンセンサスが揺さぶられているように見受けられる。

この点について検討するために、V-Dem 研究所による自由民主主義度に関するデータと、世界知的所有権機関（WIPO）によるグローバルイノベーション指数に関するデータを用いて分析してみると、両者の間には正の相関関係（r=0.61）が確認される。この結果から、現在においても引き続きイノベーションの観点からすると民主主義国の方が有利だという評価もある[7]。

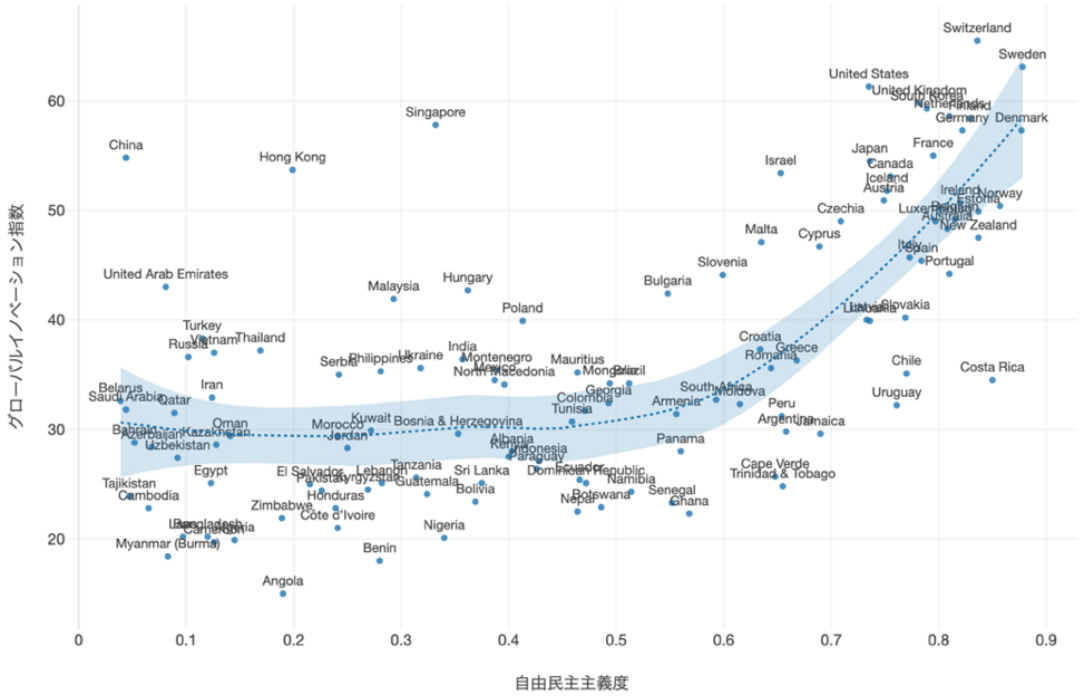

図 5-3：自由民主主義度とグローバルイノベーション指数との関係性

（出典）筆者作成。データは、V-Dem Dataset（v.12）およびグローバルイノベーション指数（世界知的所有権機関）を使用。破線は LOESS 平滑化曲線、網掛けは 95%信頼区間を示している。なお、イノベーションが期待しにくいという観点から、世界銀行の区分で「低所得国」についてはデータから除外している。

とはいえ、より詳細に分析してみると異なる景色が見えてくる。図 5-3 は、横軸を自由民主主義度、縦軸をグローバルイノベーション指数として、2021 年における各国のデータをプロットしたものである。図 5-3 が示すように、政治体制とイノベーションとの間に正の相関関係が生じるのは、概ね自由民主主義度が 0.5 を超えたあたりからである。0.5 というのは、このあたりを民主主義国と非民主主義国との閾値として考えることのできる値でもある。

この閾値で区切ってそれぞれのデータを分析してみると、政治体制とイノベーションとの関係は、自由民主主義度スコアが 0.5 以上の国では比較的強い相関関係（r=0.71）があるものの、スコアが 0.5 未満の国では無相関（r=0.01）であることがわかる。イノベーションの起こしやすさという視点からみて民主主義度が高い国ほど有利かもしれないという状況は、民主主義国の間でのみ観察される現象であって、一定の水準以下の民主主義度の国においては政治体制とイノベーションとの間に相関関係はみられない。それどころか、次節でより詳細に検討する AI に関連する分野においては、「監視国家」の度合いを強め広範囲に及ぶ国民の行動データを収集している非民主主義国は、しばしば「21 世紀の石油」とも形容されるデータ収集の点で有利だという見方もできる。

4. AI をめぐる政治体制間の競争とサイバーセキュリティ

外国勢力による選挙介入という点において、AI は厄介な技術になり得る。特に、フェイクニュースの生成と拡散は、深刻な懸念材料である。民主主義国の選挙にマイナスの影響を与えるための攻撃は、必ずしも大規模かつ派手なものである必要はない。むしろ、地味に目立たない形で、当該国の有権者たちに国内で流通する情報や民主主義への信頼を少しずつ蝕む形で行われることになるだろう。有権者たちが持つ、民主主義そのものに対する信頼を徐々に削ぎ落とすことができれば、攻撃者にとっては「成功」だと位置付けられる。

民主主義国において言論空間がオープンかつ自由であることは、民主主義社会の基本的価値として守られる必要がある。しかしながら、その開放性と自由さを維持しようとする限り、悪意を持った外国勢力による持続的な攻撃と常に隣り合わせとなる。国内的に見ても、こうした状況に対応できないと、スキャンダルに見舞われた政治家が、たとえそれが真実であっても「フェイクニュース」だと主張することで利益を得る、いわゆる「嘘つきの配当（liar's dividend）」を促す環境を増長しかねない[8]。民主主義的な基本的価値を守りつつ、サイバーセキュリティへの実効性を担保することは、これからの民主主義国にとって重要な政策課題となる。

インターネットのコントロール効率を高めるためにこれまでも様々な技術が使われてきたが、近年の AI をめぐる技術進化は状況を次の段階へと引き上げる可能性がある。インターネットの監視を行おうとする政府は、AI 技術の革新により、より検知されにくく、国民の反発を招きにくい形での正確な検閲を行えるようになっている[9]。他方、Chat GPT に代表される生成型 AI は、権威主義体制において抑圧されることの多い情報を含めてトレーニングがされており、これらが現状に風穴を開ける可能性も指摘されている[10]。

大量のデータが「21 世紀の石油」として新たな技術的なイノベーションを引き起こしたり、今ある技術の精度を高めたりする上で重要だとするならば、「監視国家」の度合いを強め広範囲にわたるデータ収集を国家レベルで推し進める権威主義体制の方が有利だとの見方がある。ただし、ヘンリー・ファレル（Henry Farrell）らの研究にあるように、現実はそれほど単純ではなく機械学習は民主主義国の政治的分断を増大させるという意味でダメージを与えうるかもしれないが、権威主義体制ではフィードバックが働きにくいことから正しい現実理解を妨げ、体制を大きく揺るがす可能性もあるとの指摘も存在する[11]。

「監視国家」の度合いが強いほど、国民が政府に対して反感や不満を募らせているかといえば、こちらもそう単純ではない。図 5-4 は、世界価値観調査（World Values Survey）における「政府は国民に知らせることなく情報を収集する権利を持つべきか」という問いに対する回答結果を示したものである。図 5-4 の左側に位置するミャンマー、パキスタン、ヨルダン、イラク、インドネシア、フィリピン、バングラデシュ、中国、イランといった国では、設問に対して肯定的な見解を示す割合が全体の半数を超えている。

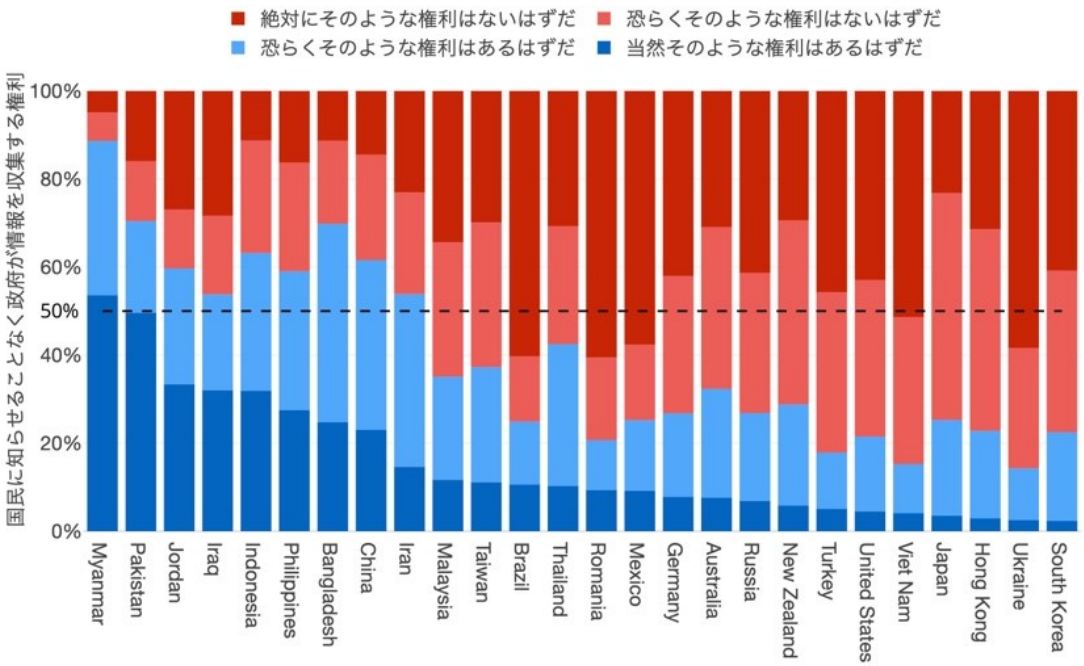

図 5-4：「監視国家」に対する認識の国際比較

（出典）筆者作成。データは、世界価値観調査（Wave 7）を使用。破線は、50%の位置を示している。

世界価値観調査には、「政府は、公共空間でのビデオ監視を実施する権利を持つべきか」、「政府はすべての電子メールおよびその他ネット上でやり取りされる情報の監視を行う権利を持つべきか」という似た設問も用意されているが、各国の特徴は全体的に図 5-4 と似たような傾向を示し、割合としては肯定的に捉える人がより増えるという結果になっている。他方、ロシア、トルコ、ベトナムなどの国は、権威主義体制でありながら図 5-4 の設問に否定的な見解を示す国民が過半数を超えている。「国家安全維持法」が施行されている香港でも、否定的な見解を示す人の割合が高い。

サイバーセキュリティの実効性を高める上で、インターネットの監視は欠かせない。初期のインターネット・コントロールは、比較的シンプルかつ人間が監視役を担うことも少なくなかった。この時代であれば、何がどう行われているのかをイメージすることもできた。ところが、AI 時代が本格化していくにつれて、インターネットの監視として何がどう行われているかの中身は、ますますブラックボックスに覆われるようになっている。

だからといって、透明化すればよいという単純な話では済まない。これからの民主主義国は、民主主義的な価値を維持しつつ、国民の民主主義的制度への信頼を侵食することなく、同時にサイバーセキュリティの実効性を担保していくという政策課題をクリアしていかなくてはならない。このバランスが維持できなくなると、「民主主義の後退」と呼ばれる現象を更に加速させてしまう可能性がある。

5. 民主主義国家への教訓

最後に、政治体制とサイバーセキュリティの観点から、有事となった際の民主主義国への教訓について考えてみたい。

図 5-2 において示したように、インターネットの自由度において「自由」、「部分的に自由」、「不自由」のいずれのカテゴリに分類される国であっても、全体的な傾向として「A：アクセスへの障害」についての向上がみられる。これは、最新の 2023 年度版において最下位の評価を受けている中国であっても例外ではない。また、前述のように、「C：ユーザーの権利の侵害」については、いずれのカテゴリにおいても悪化傾向にある。

過去 10 年超の推移を見る限り、「不自由」に分類されるような国と、それ以外の国とでの差異は、主に「B：コンテンツ制限」に踏み込んでいくか、踏み止まるかにある。この差異は、2014 年のクリミア併合をはさんでの、ロシアとウクライナとの比較でも同様のことが観察される。

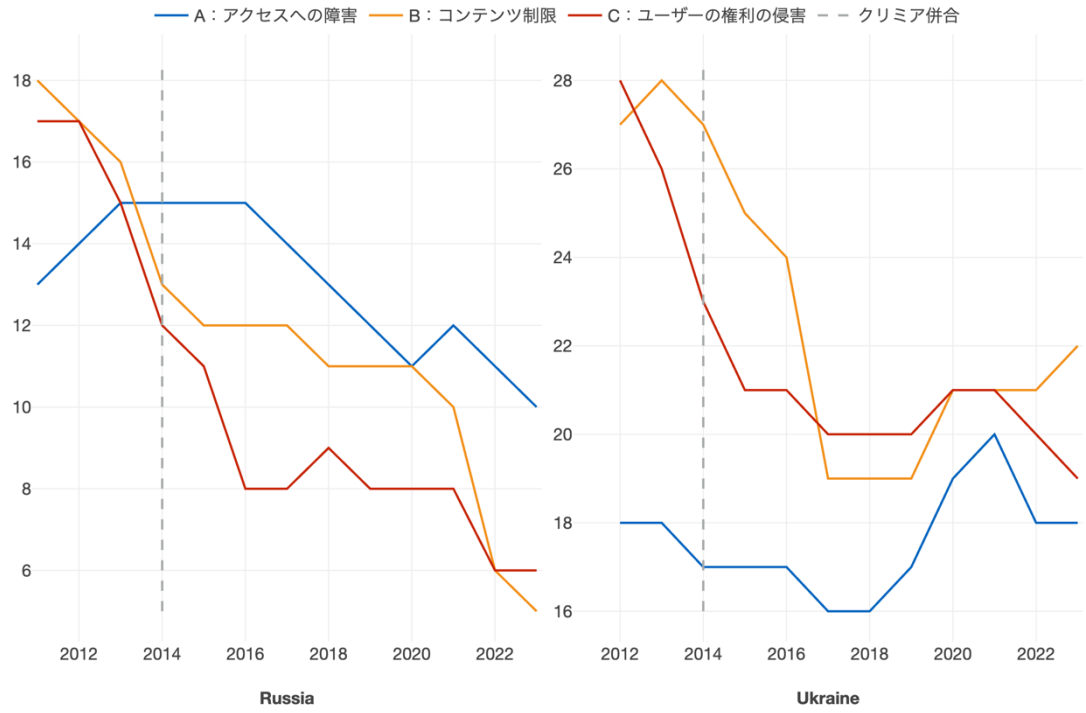

図 5-5：インターネットの自由度をめぐるロシアとウクライナの推移

（出典）筆者作成。データは、フリーダムハウスによる Freedom on the Net のスコアを使用。なお、両国の傾向を確認するという趣旨から Y 軸は同期させていない。

クリミア併合の時期を挟んでウクライナは、サイバーセキュリティ対策を強化してきたと考えられるが、ある程度「B：コンテンツ制限」および「C：ユーザーの権利の侵害」を犠牲にしつつも 2016 年頃からは横ばいないしは状況の改善がみられる。2022 年のロシア

による侵攻を受け、「C：ユーザーの権利の侵害」については数値の低下がみられるが、「B：コンテンツ制限」については数値が上昇している。

対して、ロシアの場合は、すべての分野で数値を落としている。中でも、「B：コンテンツ制限」についての落ち込みは大きく、2022 年のウクライナ侵攻以降もさらに数値を悪化させている。

より詳細に分析してみると、「B：コンテンツ制限」を構成する変数のうちロシアが特に数値を下げているのは、「オンラインの情報環境が多様性と信頼性に欠けている状況があるか」および「政治的・社会的な問題に関して、ユーザーの動員力、コミュニティ形成力、キャンペーン力を阻害するような状況があるか」への評価である。ウクライナは、この間「B：コンテンツ制限」の状況を改善させているが、その理由はロシアが数値を下げているオンライン情報環境の多様性と信頼性、およびユーザーの動員、コミュニティ形成、キャンペーンなどを阻害しているかどうかという点において評価を向上させているためである。

有事の際に、または有事に備えて、サイバーセキュリティを強化させる必要があるという点については論を待たない。その際に、何を犠牲にしてもやむを得ないと考えるか、どの点においては踏み止まるべきかは、民主主義国にとっての政策判断上悩ましい要素になるだろう。

安全かプライバシーかという議論においては、「C：ユーザーの権利の侵害」をどう避けながら政策展開していくのかが重要であるが、有事において安全寄りの判断がなされるという点については避けられない側面がある。むしろ、そのような状況下にあっても、「B：コンテンツ制限」を過度に強化することなく、情報環境の多様性と信頼性を維持し、人々の動員、コミュニティ形成、キャンペーン展開などを阻害しないように踏み止まれるかが、民主主義国にとっての評価の分かれ目になると考えられる。

国際戦略研究所（International Institute for Strategic Studies：IISS）は、サイバーセキュリティ能力に関する分析報告書において、米国を唯一「Tier1」として最高レベルのサイバーセキュリティ能力を保持していると評価している[12]。ただ、同時に「世界最高峰の能力があるが、能力の行使に際しては、ロシア、中国、イラン、北朝鮮に比べると政治的・法的な制約があるように見受けられる」との懸念も表明している[13]。この微妙なバランスの中で、有事の際にも民主主義国としての判断を保ち続けられるか否かは、「民主主義の後退」がトレンドとなっている中でのサイバーセキュリティ政策展開において、民主主義国としての価値が試される正念場になると言えよう。

[1] Larry Diamond, “Facing Up to the Democratic Recession,” *Journal of Democracy*, Vol.26, No.1, 2015, pp. 141-155.

[2] Yascha Mounk, “Democracy on the Defense: Turning Back the Authoritarian Tide,” *Foreign Affairs*, Vol. 100, No.2, 2021, pp.164-174.

[3] たとえば、以下の書籍を参照されたい。Jamie, Bartlett, *The People vs Tech: How the Internet is Killing Democracy (and How We Save It)*, Penguin Random House, 2018（秋山勝訳『操られる民主主義：デジタル・テクノロジーはいかにして社会を破壊するか』草思社、2018 年）.

[4] 土屋大洋、川口貴久『ハックされる民主主義：デジタル社会の選挙干渉リスク』千倉書房、2022 年。

[5] Funk Shahbaz, Brody Vesteinsson, Baker Grothe, Barak Masinsin, and Modi Sutterlin eds. *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence*, Freedom House, 2023, p.2.

[6] 厳密には、ラテンアメリカ・カリブ海地域のみ、回帰直線が右肩上がりの方向を示すことになるが、これはインターネットの自由度スコアが 85 を超えるようなコスタリカが 2021 年より調査対象国に入った影響による。図 1 は、コスタリカをデータから除いて分析した結果である点に留意されたい。

[7] Simon Commander, Saul Estrin, and Thamashi De Silva, “Political Systems Affect Innovation,” *London School of Economics Business Review*, 2022, https://blogs.lse.ac.uk/businessreview/2022/04/05/political-systems-affect-innovation/, accessed November 12, 2023.

[8] Kaylyn Jackson Schiff, Daniel S. Schiff and Natalia Bueno, “The Liar's Dividend: The Impact of Deepfakes and Fake News on Trust in Political Discourse,” *SocArXiv x43ph*, Center for Open Science, 2023, https://ideas.repec.org/p/osf/socarx/x43ph.html, accessed November 12, 2023.

[9] Funk Shahbaz, Brody Vesteinsson, Baker Grothe, Barak Masinsin, and Modi Sutterlin eds. *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence*, Freedom House, 2023, p.13.

[10] *Ibid.*, p.13.

[11] Henry Farrell, Abraham Newman, and Jeremy Wallace, “Spirals of Delusion: How AI Distorts Decision-Making and Makes Dictators More Dangerous,” *Foreign Affairs*, Vol. 101, No. 5, 2022, pp. 168-181.

[12] IISS, *Cyber Capabilities and National Power: A Net Assessment*, The International Institute for Strategic Studies, 2021.

[13] *Ibid.*, p.9.

第 6 章
提言：台湾有事への備え

土屋 大洋、川口 貴久、佐々木 孝博、八塚 正晃、山本 達也

本報告書は、作戦領域の拡大、ロシア流の戦争、中国による学習、テック企業の関与、政治体制等の観点から、ウクライナ戦争での教訓、将来の台湾有事への適用を検討した。これらを踏まえ、また第 1 章から第 5 章まで論じていない事項を含めて、将来の台湾有事の備えとして以下の点を提案する。これらは台湾有事への備えとして必要な事項を網羅するものではないが、筆者らが優先度の高い課題として認識するものである。

- 全般： 先端技術の防衛分野への適用・実装の迅速化
- 全般： テック企業との協力と連携
- 宇宙領域： 多軌道衛星通信を含む有事の通信レジリエンスの向上
- サイバー・認知領域： 一元化された状況認識・対処体制の確立
- サイバー領域： 「積極的サイバー防御」体制の早期実現
- 認知領域： プラットフォーム上の状況認識能力の強化（認知戦の「守り」）
- 認知領域： 戦略的コミュニケーションの強化（認知戦の「攻め」）
- 電磁波領域： グレーゾーン事態・有事を想定した電磁波管理
- 伝統的領域との融合： 無人機作戦への備え

全般： 先端技術の防衛分野への適用・実装の迅速化

- 【教訓】 ウクライナ戦争では様々な先端技術が活用された。ウクライナによる AI の軍事活用は指揮統制だけでなく、無人機部隊、無人艦隊、認知電子戦、顔認証による工作員の判別など多岐に渡る。
- 【提言】 民間セクターを中心に開発された先端技術を迅速に防衛分野で検証・試行・開発・実装していく必要がある。例えば、北大西洋条約機構（North Atlantic Treaty Organization: NATO）では 2021 年 6 月、革新的技術を迅速に防衛分野で実装するた

めのプログラム「NATO 防衛技術革新アクセラレーター（Defence Innovation Accelerator for the North Atlantic: DIANA, 通称ダイアナ)」の設置を発表した。日本では 2015 年、防衛装備庁が先端的な基礎研究に資金を提供する「安全保障技術研究推進制度」が創設されたが、よりタイムスパンの短い投資・検証・開発が必要である。

全般： テック企業との協力と連携

- 【教訓】 ウクライナ戦争におけるサイバー領域の攻防では、ウクライナ自身の投資と試みに加えて、アマゾン、グーグル、スペース X、マイクロソフト等の米欧のテック企業が重要な役割を果たした。認知領域や宇宙領域でも同様の役割が確認できる。しかし、中国が関与する台湾有事では、紛争の構造、東アジアの通信インフラ環境、中国に関する蓄積という観点で、こうしたテック企業が同様の関与と効果を果たせるかは疑わしい。
- 【提言】 今後、将来の紛争を想定し、新領域の防衛に資する国内外のテック企業同盟・有志連合を形成するため、ルール整備・戦略的提携を進めるべきである。具体的には、以下の施策（例）が考えられる。
  - テック企業の防衛行動に関する国際法上・国内法上の位置づけを明確化する
  - 新領域の防衛に資するテック企業、特に台湾有事に貢献しうるテック企業への財政面・情報面等での支援を行う
  - 将来の潜在的紛争についてテック企業等の意思決定・判断の材料となる基本的認識（例：仮に中国が台湾を強制的手段によって統一を試みた場合の日本や同盟国・有志国の認識等）を同盟国・有志国とともに継続的に発信する
  - 政府や民間シンクタンクが実施する War Game やシミュレーションにテック企業の参加を促す

宇宙領域： 多軌道衛星通信を含む有事の通信レジリエンスの向上

- 【教訓】 ウクライナ戦争では、スペース X 社による低軌道衛星コンステレーション通信サービス「スターリンク」が、ウクライナ政府・軍にとって決定的な役割を果たしていると同時に、スターリンクに依存することのリスクが明らかになった。四方を海に囲まれた台湾では、ウクライナ以上に衛星通信が重要な役割を果たすと考えられる。また通信に加えて、測位・航法・計時（Positioning, Navigation, and Timing: PNT）機能、具体的なサービスとしては GPS の重要性が明らかになった。中国もウクライナ戦争におけるロシアの GPS 妨害を学んでいるとみられる。
- 【提言】 先行する台湾の取組みを参照しつつ[1]、日本は外国資本を含め、異なる軌道の衛星通信プロバイダとの提携を通じて、有事における通信レジリエンスを向上させるべきである。異なる軌道や異なる（国の）プロバイダとの衛星通信を確保すれば、有事の通信レジリエンスは向上する。しかし、これはコストに直結するため、政治的な投資

判断が求められる。

サイバー領域： 「妨げる能力」「積極的サイバー防御」の早期実現

- 【教訓】 ロシアはウクライナ全面侵攻初期、相当なリソース（資金、要員、時間、技術的資産等）を投入した。しかし、2014 年以降のウクライナ自身のサイバー防衛への投資や開戦後の対応（ロシアへの攻撃的サイバー作戦を含む）、米国サイバー軍（U.S. Cyber Command: USCYBERCOM）の「ハントフォワード」作戦やテック企業の支援によって、これまでのところウクライナはサイバー戦の防衛に成功している。また中国も有事を念頭に重要インフラ（エネルギー、通信、交通・物流等）への破壊的・妨害的能力を向上させているとみられる。こうしたサイバー攻撃を効果的に防ぐには、純粋に防衛的なサイバー作戦は限界がある。
- 【提言】 日本のサイバー安全保障戦略では、有事においては「我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力」（『防衛大綱』、2018 年 12 月 18 日閣議決定）を行使し、武力攻撃に至らないグレーゾーン事態では脅威を未然に排除し、被害拡大を防止する「能動的サイバー防御（active cyber defense: ACD）」（『国家安全保障戦略』、2022 年 12 月 16 日閣議決定）を確立する、としている。前者の「妨げる能力」は有事に限定されているが、「妨げる能力」を有事に行使するためには、平時からの偵察・情報収集活動が不可欠である。また現時点で ACD の内容や目指すべき姿について明確な共通理解はないものの、『国家安全保障戦略』の内容を踏まえると、ACD は政府の管理下にあるネットワークや情報資産の"外側"での活動を含む。

サイバー・認知領域： 一元化された状況認識・対処体制の確立

- 【教訓】 ロシアや中国はその戦略やドクトリンで、サイバー領域と認知領域の戦いを一体的に位置付けているとみられる。事実、ロシアはウクライナ全面侵攻の前後、心理的効果を狙ったとみられるサイバー攻撃を展開した。サイバー戦と認知戦の一体的運用といえる。
- 【提言】サイバー戦と認知戦を一体的に対応できる体制を確立すべきである。その体制は、①各省庁の関心と特徴に基づく対応体制は維持しつつ、省庁横断的な状況認識・対処体制（内閣官房等）、②外国資本を含むプラットフォーマー、ファクトチェック機関、サイバーセキュリティ企業等との官民連携体制、③既存のサイバー攻撃やキネティックな事態対処に加えて、平時、グレーゾーン、有事の認知戦を迅速に検知・対処できる体制のすべてを満たすことが期待される。

認知領域： プラットフォーム上の状況認識能力の強化（認知戦の「守り」）

- 【教訓】 ウクライナ戦争や各国の台湾有事シミュレーションを踏まえると、台湾有事では台湾、米国、日本が認知戦のターゲットとなる可能性が高い。こうした認知戦は党・政府の支配・影響下のメディアによって行われるものに加えて、発信者を偽装する形で、様々なデジタルプラットフォーム（DPF）上で展開される。米国際問題戦略研究所（CSIS）のシミュレーションによれば、中国が台湾侵攻を成功させる２つの条件とは、「米国が関与せず、台湾独力での対応となった場合」と「日本が中国の圧力に屈し、在日米軍基地の使用などで米軍を支援しなかった場合」である[2]。そのような観点からすると、「我が国における日米同盟に対する否定的な世論形成や米国における台湾関与に関する否定的な世論形成のための情報戦を考慮」する必要性がある。
- 【提言】 有事の認知戦・情報戦に対処する場合、市民や国民の自由な発信や表現を制限することなく、外国政府に起因する意図的な干渉のみを対象とすることが不可欠である。こうした外国からの認知戦・情報戦を検知・分析・対処するため、DPF と協力・連携を進めるべきである。特に外国資本の DPF の協力が得られない場合、欧州デジタルサービス法（Digital Service Act: DSA）では一定規模以上の DPF に危機時の協調を要請し、またウクライナ戦争では DPF 上の外国政府系メディアの活動・発信を禁じたことを参考にしつつ、共同規制や直接規制も考慮すべきである。

認知領域： 戦略的コミュニケーションの強化（認知戦の「攻め」）

- 【教訓】ウクライナ戦争初期では、ゼレンスキー政権による国内外向けの戦略的コミュニケーションが、ウクライナ軍・市民の士気を高め、米欧によるウクライナ支援を引き出し、ロシアに強力な経済制裁を課した。中国は台湾有事を念頭に、平時における外交攻勢や世論戦を重視しており、とりわけ、「一つの中国原則」についての国際的な言説を自国優位に構築することを図っている。その中でも、ウクライナ戦争において中立性を保つ発展途上国・新興国（グローバル・サウス）に対する外交的取り込みや情報プラットフォームの輸出、メディア買収などを含むパブリック・ディプロマシーを強化している。
- 【提言】 先進諸国だけでなく発展途上国・新興国（グローバル・サウス）の外交当局者に対する東アジア情勢、台湾海峡に関する情報発信やブリーフィングの強化、同地域メディアに対する専門家による寄稿の活性化への各種支援を行うべきである。また、台湾 有事に備え、グローバル・サウス諸国で影響力を有する SNS プラットフォームにおいて政府見解を発信できる有力なアカウントを保持し、平時から多数のフォロワーを獲得し、発信力の強化を図るべきである。

電磁波領域： グレーゾーン事態・有事を想定した電磁波管理

- 【教訓】 第 2 章でロシアの実行した電磁波領域の戦いについて言及したが、伝統的な陸海空の領域における戦いを優位に進めるために、中国もその有用性や問題点を学んでいる。ロシアが成功した手法（GPS の妨害や電子攻撃でウクライナ側のミサイルやドローンの追尾を外す例や携帯電話を乗っ取り情報戦を実施した例など）は取り入れるであろうし、失敗した事例（妨害電波に追尾するようなミサイルやドローンをウクライナ側が使用したことにより被弾してしまった例など）は改善していくものとみられる。
- 【提言】 電磁波領域での戦いは、平時有事を問わずに行われる。そのような観点で、我が国は平時において、総務省が電波管理・割り当て等を行っており、有事とは必ずしも位置づけられないグレーゾーン事態において、軍事安全保障に必要な電波が優先的に使用できる環境にはない。それを是正していく必要性がある。また、有事においても、軍事に必要な電磁波攻撃が、通常の市民生活に必要な電磁波の使用に影響を及ぼす可能性がある場合それをどこまで許容するのか、どのような手段で行うのか、どの組織がそれを決定するのかなどが明確には定められていない。電磁波の運用について、平時とは異なった判断・統制・調整ができる国家的な枠組みを構築していく必要がある。

伝統的領域との融合： 無人機作戦への備え

- 【教訓】中国人民解放軍は、将来戦である「智能化戦争」において戦闘の無人化を念頭に無人機作戦の増加を予想する中で今回のウクライナ戦争でも無人機作戦の有用性を確認し、周辺海域において無人機運用を活発化させるとともに、台湾有事に向けて無人機作戦の実施体制の整備や実戦配備を強化している。
- 【提言】中国人民解放軍による周辺地域における無人機の運用や能力、将来の見通しについての包括的調査・研究を実施するとともに、海上保安庁・自衛隊による対処要領を策定し、電磁妨害などを含めた対処能力の向上を図るべきである。また、無人機作戦に関して米国や同志国との連携を強化するとともに、海上・海中・空中における軍用無人機の安全な運用や遭遇対処に関する国際規範の形成へ取り組みを強化するべきである。

[1] ウクライナ戦争や台湾本島-馬祖列島の海底ケーブルの切断事故をふまえて、台湾政府は非常時の衛星通信レジリエンスの向上に取り組む。具体的には、台湾は独自の低軌道通信衛星の打ち上げ、複数の衛星通信プロバイダと提携可能な地上設備の整備（携帯基地局のバックホールを含む 773 施設を設置予定）、外国資本の低軌道衛星通信プロバイダ（Eutelsat OneWeb）および静止衛星・中軌道衛星通信プロバイダ（SES 社）との提携を進める。唐鳳（Audrey Tang）デジタル発展部長によれば、「（台湾政府が）複数の衛星プロバイダに投資するのは単に冗長性のためではない」「多くの管轄権、多くの国のシステムと協力することを望んでいる。結果、異なる国に帰属する異なる衛星システム全てを同時にジャミングしたり、妨害することは非常に難しくなくなる」とみる。要は、同時多発的なキネティックおよびサイバー攻撃に耐えうる態勢を構築しようとしている。
Kelvin Chen, “Taiwan ramps up efforts to finish backup satellite network: Digital Minister Audrey Tang says Taiwan diversifying its satellite providers,” Taiwan News, September 23, 2023.

[2] Mark F. Cancian, Matthew Cancian, and Eric Heginbotham, The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan, Center for Strategic and International Studies (CSIS), January 9, 2023.

著 者 紹 介

土屋 大洋（慶應義塾大学大学院政策・メディア研究科教授）

1999 年 3 月、慶應義塾大学大学院政策・メディア研究科後期博士課程修了。博士（政策・メディア）。日本経済新聞社客員論説委員（2019 年 4 月から現在）、経済安全保障に関する有識者会議構成員（2021 年 11 月から 2022 年 2 月、2022 年 7 月から現在）、サイバーセキュリティ戦略本部本部員（2023 年 2 月から現在）、米 National Bureau of Asian Research（NBR）Nonresident Fellow（2022 年 1 月から現在）等を兼任。著作に、『サイバーグレートゲーム：政治・経済・技術とデータをめぐる地政学』（千倉書房、2020 年）、『暴露の世紀：国家を揺るがすサイバーテロリズム』（KADOKAWA、2016 年）、『サイバーセキュリティと国際政治』（千倉書房、2015 年）等多数。

川口 貴久（東京海上ディーアール主席研究員）

慶應義塾大学グローバルリサーチインスティトュート（KGRI）特任准教授（2023 年 11 月から現在）を兼任。1985 年、福岡県生まれ。専門は国際政治・安全保障、リスクマネジメント。2008 年 3 月、横浜市立大学国際文化学部国際関係学科卒業。2010 年 3 月、慶應義塾大学大学院政策・メディア研究科修了。近著に『ハックされる民主主義：デジタル社会の選挙干渉リスク』（土屋大洋との共編著、千倉書房、2022 年）等多数。これまで一橋大学大学院法学研究科非常勤講師（2022 年 4 月から 9 月、2023 年 4 月から 9 月）、慶應義塾大学 KGRI 客員所員（2021 年 6 月から 2023 年 6 月）等を兼任。

佐々木 孝博（広島大学法学部客員教授）

広島大学法学部客員教授、東海大学平和戦略国際研究所客員教授、明治大学サイバーセキュリティ研究所客員研究員、博士（学術）〔広島大学〕。1986(昭和 61)年、防衛大学校（電気工学）卒業後、海上自衛隊に入隊。その後、米海軍第 3 艦隊司令部連絡官、オーストラリア海軍大学留学、護衛艦ゆうべつ艦長、在ロシア防衛駐在官、第 8 護衛隊司令、統合幕僚監部サイバー企画調整官、指揮通信開発隊司令、下関基地隊司令などを経て、2018 年に防衛省を退官（海将補）。単著に『近未来戦の核心サイバー戦－情報大国ロシアの全貌』（育鵬社）、共著に『現代戦争論－超「超限戦」』（ワニブックス PLUS 新書）、『プーチンの超限戦』（ワニプラス）、『ネット世論操作とデジタル影響工作』（原書房）等多数。

八塚 正晃（防衛研究所地域研究部中国研究室主任研究官）

1985 年、大阪府生まれ。専門は、中国政治外交（史）、東アジア国際関係論、国際安全保障論。2008 年 3 月、慶應義塾大学総合政策学部卒業。2016 年 3 月、慶應義塾大学法学研究科後期博士課程単位取得退学。北京大学国際関係学院留学（2009-2010 年）、日本学術振興会特別研究員（DC1）、香港総領事館専門調査員などを経て現職。その間、防衛省防衛政策局国際政策課部員、法政大学法学部兼任講師、オーストラリア戦略政策研究所（ASPI）客員研究員等を兼任。著作に（共著）加茂具樹（編著）『中国は「力」をどう使うのか』（一藝社、2023 年）、（共著）川島真・小嶋華津子（編著）『習近平の中国』（東京大学出版会、2022 年）等多数。

山本 達也（清泉女子大学文学部教授）

1975 年、東京都生まれ。慶應義塾大学大学院政策・メディア研究科後期博士課程修了。博士（政策・メディア）。シリア国立アレッポ大学学術交流センター主幹、慶應義塾大学 SFC 研究所上席所員、名古屋商科大学コミュニケーション学部准教授等を経て現職。専攻は、国際関係論、公共政策論、民主主義論。著書に、『革命と騒乱のエジプト：ソーシャルメディアとピーク・オイルの政治学』（慶應義塾大学出版会）、『暮らしと世界のリデザイン：成長の限界とその先の未来』（花伝社）、『地域間共生と技術：技術は対立を宥和するか』（共著、早稲田大学出版部）、『ポスト・グローバル化と政治のゆくえ』（共著、ナカニシヤ出版）等多数。