中国が目指す非接触型「情報化戦争」
――物理領域・サイバー領域・認知領域を横断した「戦わずして勝つ」戦い――

荊　元宙・五十嵐　隆幸

＜要旨＞

中国のサイバー領域における活動は、「軍民融合」路線の下、人民解放軍のみならず、国家規模で多方面にわたって繰り広げられるようになっている。また、古くから認知領域での闘争を重視してきた中国は、新興メディアの普及を背景に、新旧メディアをパッケージ化した戦い方へと変化している。その中国は、物理領域、サイバー領域、認知領域といった3つの領域を横断し、敵と接触せずに目的を達成する「情報化戦争」の能力構築を目指している。例えば、2022年8月のペロシ米下院議長の訪台前後、サイバー攻撃や軍事演習に合わせ、台湾の人々の心に揺さぶりをかけるディスインフォメーションが台湾社会に流布された。だが、台湾の人々が中国の軍事的な威嚇行為などに慣れてしまっていたため、中国が求める効果は十分に得ることができなかった。今日、台湾は中国が領域横断的な非接触型「情報化戦争」の能力を国家総動員で構築していくための「試験場」になっている。

はじめに

中国は、2015年5月に発表した国防白書『中国の軍事戦略』において、胡錦濤時代に提起された「情報化[1]条件下での局地戦争における勝利」を目標とする軍事戦略の方針を発展させ、軍事闘争準備の重点を「情報化局地戦争における勝利」に据えることを明らかにした[2]。この「情報化局地戦争」の特徴として、中国人民解放軍（以下、人民解放軍）の国防大学に所属する研究者などによって同年4月に出版された『戦略学』では、戦場空間の大幅な拡大をその一つに挙げている。同書では、陸、海、空、宇宙などの有形の戦場に加え、電磁スペクトラム、サイバー空間、心理・認知領域な

1　原文の中国語では「信息化」だが、本稿ではそれを「情報化」と訳して用いる。中国語では、ただ伝え聞いてそのままの状態の情報（生の情報、information）を「信息」と言い、信憑性を吟味したうえで解釈を施した情報（加工された情報、intelligence）を「情報」と言うが、日本語ではどちらも「情報」と表現している。本稿が指す「情報」とは、特に断らない限り「信息」（information）を意味する。

2　中華人民共和国国務院新聞弁公室「中国的軍事戦略」『人民日報』2015年5月27日。

どの無形の戦場へと戦場空間が広がり、さらにそれら領域間を横断した非線形的作戦（Non-linear Operations: NLO）が繰り広げられ、敵と接触することのない作戦をも起こりうると説明されている[3]。

この 2015 年版『戦略学』で示された領域横断的な作戦と同様の概念は、2012 年 1 月に米国防省が発表した「統合作戦アクセス構想（Joint Operational Access Concept: JOAC）」において、その中心的な考え方として「領域横断的な相乗作用（Cross Domain Synergy: CDS）」が示されたのち[4]、日本や NATO 諸国でも同様の概念が案出されてきた。近年では、多くの国の軍隊で CDS について盛んに議論が繰り広げられているが、その概念について、中国やロシアは然ることながら、米国をはじめとする NATO 諸国や日本においても共通の認識が確立されておらず、ひいては個人ごとにも異なるイメージが抱かれている。ただし、「領域」についての認識は、米国や NATO 諸国のみならず、中国でもほぼ共通しており[5]、本稿では CDS の区分を準用し、物理次元に存在する陸、海、空、宇宙の 4 領域は「物理領域」、情報次元は Information と Intelligence との混同を避け、かつ、実態にそぐわせて「サイバー領域」、人間の心の中を「認知領域」として議論を進めていく。

2012 年の JOAC 発表後、多くの国の軍隊で CDS に対する関心が高まるなか[6]、飯田

3　肖天亮主編『戦略学』（北京：国防大学出版社、2015 年）164–166 頁。また、廣瀬陽子によると、ロシアのウラジミール・スリプチェンコ少将が第 6 世代の戦争がハイテク型の「非接触型」の戦争になると予言し、ウラジスラフ・スルコフ元大統領補佐官がこれからの戦争を「非線形戦争」と呼んだと説明している（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、2021 年）38–40 頁）。

4　Department of Defense, *Joint Operational Access Concept (JOAC)*, Version 1.0, January 17, 2012.

5　CDS を提起した米国の認識は、統合参謀本部が軍事作戦下の情報作戦（Information Operations）のために示した統合ドクトリンによると、情報の収集、処理、拡散、作用に関わるシステム（情報環境）ごとに、それらの領域を「物理次元（Physical dimension）」、「情報次元（Informational dimension）」、「認知次元（Cognitive dimension）」の 3 つに区分している。同ドクトリンによると、陸・海・空・宇宙の 4 領域は物理空間に存在することから「物理次元」、サイバー領域は仮想空間に存在することから「情報次元」、そして人間の心の中が「認知次元」と区分されている（Joint Chiefs of Staff, *Information Operations (Joint Publication 3-13), Incorporating Change 1*, Joint Chiefs of Staff, November 20, 2014, https://irp.fas.org/doddir/dod/jp3_13.pdf）。英国でも米国とほぼ同様に「物理次元」、「仮想次元（Virtual dimension）」、「認知次元」の 3 つに区分されている（Ministry of Defence, *Defence Strategic Communication: an Approach to Formulating and Executing Strategy (Joint Doctrine Note 2/19)*, The Development, Concepts and Doctrine Centre, April 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804319/20190523-dcdc_doctrine_uk_Defence_Stratrategic_Communication_jdn_2_19.pdf）。

6　2012 年の JOAC 発表後、統合参謀本部が CDS のプランナーズガイドを公表し、各軍種の作戦構想にも CDS が取り入れられた（Joint Chiefs of Staff, *Cross-Domain Synergy in Joint Operations: Planner's Guide*, Joint Chiefs of Staff, January 14, 2016, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230）。日本でも 2018 年 12 月 18 日に閣議決定された『平成 31 年度以降に係る防衛計画の大綱について（30 大綱）』で「領域横断作戦」という概念が示され、それらに関する研究も進められている（William O. Odom and Christopher D. Hayes, "Cross-Domain Synergy: Advancing Jointness," *Joint Force Quarterly*, vol. 73, 2014, pp. 123–128; 菊地茂雄「米陸軍・マルチドメイン作戦（MDO）コンセプト―『21 世紀の諸兵科連合』と新たな戦い方の模索―」『防衛研究所紀要』第 22 巻第 1 号（2019 年 11 月）16–58 頁など）。

将史は2000年代初頭から中国が認知領域の重要性を認識していたと指摘する[7]。たしかに、2003年8月26日付の『解放軍報』に掲載された情報化戦争における認知領域に関する論評では、「将来の情報化戦争は、物理領域、情報領域、認知領域の3つの領域で同時に発生する」が、戦争の情報化の程度が高まるにつれて「認知領域の地位が拡大し高まる」と記されている。その論評によると、中国は3つの領域すべてで優勢を獲得することが重要だとしつつも、認知領域での優勢を獲得することで、初めて物理領域と情報領域における優勢をより発揮することができると主張する[8]。

また、JOAC発表とほぼ同時期、南京政治学院副教授の逯記選は「現代の戦争空間は、物理、情報、認知の3大領域から形成され、そのなかでも認知空間は主に人間の心理、論理的思考、価値観、精神面での知覚などから構成される」と説明した[9]。そしてJOAC以降、CDSについて議論が繰り広げられるなか、人民解放軍陸軍研究院の路紅衛は、現代の戦争は物理領域、情報領域、認知領域からなる「全領域」で行われるようになり、そのなかでも認知領域は、物理領域と情報領域での破壊と操作だけではコントロールすることができないイデオロギーやアイデンティティーといった新たな問題に対処する必要性から、陸上、海上、航空、宇宙、電磁スペクトラム、サイバー空間に続く対決空間になったと論ずる[10]。その認知空間で繰り広げられる対抗作戦では、文化的コミュニケーションや世論誘導などの手段によって、敵の認知領域を破壊すると同時に自らの認知領域を防御することで、主導権と支配権を確保することが目指される。この「認知対抗」の核心的な理念は、指揮官の決定能力と抵抗意思を低下させ、敵の抵抗能力の喪失を図ることにあるという[11]。

さらに近年、人工知能（AI）など新興技術を駆使した「智能化戦争」への移行が取り沙汰されている。2017年に改訂された『戦略学』では、「智能化領域での軍事競争」が新たな領域における軍事闘争の1つとして追加された[12]。2019年の国防白書『新時代における中国の国防』では、2015年の国防白書で「情報化戦争への変化を加速している」と示していた戦争形態の認識について、「戦争の形態は急速に情報化戦争へと移り変わり、智能化戦争の端緒が見えている」という表現に更新されている[13]。この中国の認識の変化に呼応するように、新米国安全保障センターのエルサ・カニア（Elsa

7　飯田将史「中国が目指す認知領域における戦いの姿」『NIDSコメンタリー』第117号（2021年6月29日）http://www.nids.mod.go.jp/publication/commentary/pdf/commentary177.pdf。
8　陳炳焱「解読信息化戦争的認知：推進中国特色軍事変革的一個新視点」『解放軍報』2003年8月26日。
9　逯記選『心戦之巔的光芒：現代戦争中的認知域作戦研究』（瀋陽：白山出版社、2012年）1頁。
10　路紅衛「再談現代戦争的本質特征」『国防』2019年第5期、16–17頁。
11　李義「認知対抗：未来戦争新領域」『人民日報』2020年1月28日。
12　肖天亮主編『戦略学（2017年修訂）』（北京：国防大学出版社、2017年）173–179頁。
13　中華人民共和国国務院新聞弁公室「新時代的中国国防」『人民日報』2019年7月25日。

B. Kania）らによって中国における AI の軍事利用の動向や「智能化戦争」について活発に議論が行われている[14]。ただし、杉浦康之は、2021 年時点で人民解放軍は智能化戦争を情報化戦争に替わる軍事ドクトリンとして設定しておらず、現時点では情報化戦争に加え、智能化戦争にも対応し得る統合作戦構想の検討に着手している段階だと主張する。さらに杉浦は、2020 年に改訂された『戦略学』では、2015 年版と 2017 年版で掲げられていた「一体化統合作戦」概念をアップデートする形で「多領域一体統合作戦」概念が登場したことを挙げ、人民解放軍は智能化戦争を視野に入れつつも、現時点では多領域での統合作戦を目指していると指摘する[15]。

なお、杉浦は、中国では他にも「領域横断統合作戦」構想など多くの概念が登場しているが、それらの定義は曖昧であり、軍内でコンセンサスを形成しているかは定かでないと説明する[16]。軍事のほかに様々な分野を組み合わせる戦いとして注目されている「超限戦」も、人民解放軍の研究者が新たな戦争モデルとして提唱した造語であり、軍の公式概念ではない[17]。また、山口信治らが指摘するように、中国は「サイバー戦」を単独のカテゴリーとして扱わず、むしろサイバーと電磁スペクトラム、そして心理戦を一体的に情報戦として捉えているといった見方もある[18]。この指摘を「領域」の区分で整理すると、物理領域を除く情報領域と認知領域で戦う方法を案出することができれば、2015 年の『戦略学』で説明されている「敵と接触することのない作戦」も起こり得るということになる。まさに、それは孫子が究極的な兵法として説く「戦わずして人の兵を屈する」戦い方と言えよう。

ここまで主要な先行研究を概観してきたが、少なくない専門家が中国の「将来の戦争」に関心を抱き、それについて議論を繰り広げている。また、2014 年のロシアによるク

14 Elsa B. Kania, “Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power,” *Center for a New American Security* (November 2017), pp. 1–73; Elsa Kania, “Learning Without Fighting: New Developments in PLA Artificial Intelligence War-Gaming,” *China Brief*, vol. 19, no. 7 (April 2019), pp. 15–19; 浅野亮「中国の知能化戦争」『防衛学研究』第 62 号（2020 年 3 月）19–41 頁；飯田将史「人民解放軍から見た人工知能の軍事に対するインパクト」『安全保障戦略研究』第 1 巻第 2 号（2020 年 10 月）1–14 頁；八塚正晃「人民解放軍の智能化戦争」『安全保障戦略研究』第 1 巻第 2 号（2020 年 10 月　）15–34 頁；Chris Bassler, “China’s Ambitions for AI-Driven Future Warfare,” Center for Strategic and Budgetary Assessments, January 1, 2022, https://csbaonline.org/about/news/chinas-ambitions-for-ai-driven-future-warfare; 荊元宙、五十嵐隆幸「中国が目指すインテリジェント化戦争―“A2/AD”作戦をモデルケースとした AI 活用についての考察―」『防衛学研究』第 66 号（2022 年 3 月）3–28 頁。

15 杉浦康之『中国安全保障レポート 2022―統合作戦能力の深化を目指す中国人民解放軍―』（防衛研究所、2021 年）22–25 頁。

16 同上、25 頁。

17 Josh Baughman, “‘Unrestricted Warfare’ is Not China’s Master Plan,” China Aerospace Studies Institute, April 25, 2022, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20Articles/2022-04-25%20Unrestricted%20Warfare%20is%20not%20China's%20master%20plan.pdf; 防衛研究所編『中国安全保障レポート 2021―新時代における中国の軍事戦略―』（防衛研究所、2020 年）18–19 頁。

18 山口信治編『中国安全保障レポート 2023―認知領域とグレーゾーン事態の掌握を目指す中国―』（防衛研究所、2022 年）18–19 頁。

リミア侵攻以降、ロシアの「ハイブリッド戦争」への関心が高まり、それに関する研究成果も数多く発表され[19]、その事例を参照して中国の「ハイブリッド戦争」を考察する試みも増えている[20]。他方、中国は伝統的に「ハイブリッド戦争」の概念と重なる「政治戦争」を繰り広げており、敵対する国が「ハイブリッド戦争」を仕掛けてくることに対応するため、それを研究しているとも指摘されている[21]。しかし、「ハイブリッド戦争」という言葉は、ロシアの軍事ドクトリンその他で正式に採用されておらず[22]、それに関する認識・理解は非常に多様で、画一的な定義はほぼ不可能である[23]。とは言うものの、このような活発な議論は、1990 年代以降の持続的な経済成長を背景に軍事力の増強を続ける中国への関心の高まりを表しているといっても過言ではない。これら研究成果の多くは、米国ランド研究所のレポートで「人民解放軍には最近の戦闘例がないため、中国共産党の戦略指針に従って策定された作戦コンセプトが、人民解放軍がどのように戦うのかを占う最良の指標となる」と示されているように[24]、『戦略学』など人民解放軍の教範類や、中国の専門家が『解放軍報』に寄稿した論考などをから「将来の戦争」を洞察しようとするものである。

だが、2021 年 11 月に発表された台湾の『国防報告書』によると、中国は台湾に対する海軍艦艇や空軍機による圧力に加え、サイバー戦と認知戦を駆使し、「戦わずに台湾を占領する」という目標達成に動いていると説明されている[25]。つまり、中国は「戦争」に至らない状況で、物理領域、サイバー領域、認知領域といった領域を横断し、接触せずに目的を達成する「情報化戦争」を既に繰り広げているのである。中国が真に「戦わずして人の兵を屈する」ことを目指すのであれば、いわゆる戦時に至らない「グレーゾーン」で繰り広げられている行動を分析する意義は大きく、かつ、中国の「将来の戦争」を考察するうえでも、台湾に対する中国の「敵と接触することのない作戦」は重要な事例だと言えよう。

19 Williamson Murray and Peter R. Mansoor eds., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, (New York: Cambridge University Press, 2012).

20 Ross Babbage, “Stealing a March: Chinese Hybrid Warfare in the Indo-Pacific; Issues and Options for Allied Defense Planners,” Center for Strategic and Budgetary Assessments, July, 2019; Laris Gaiser, “Chinese Hybrid Warfare Approach and the Logic of Strategy,” *National Security and the Future*, vol. 23, no.1, 2022, https://doi.org/10.37458/nstf.23.1.3.

21 Derek Solen, “Fight Fire with Fire: The PLA Studies Hybrid Warfare,” China Aerospace Studies Institute, March 23, 2022, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20Articles/2022-03-23%20Fight%20Fire%20with%20Fire.pdf?ver=5LsQVgQEt53Er0kLTyn0zQ%3D%3D.

22 小泉悠「ウクライナ危機にみるロシアの介入戦略―ハイブリッド戦略とは何か―」『国際問題 1』第 658 号（2017 年 1･2 月）40 頁。

23 廣瀬陽子『ハイブリッド戦争』337–341 頁。

24 Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, “Pepole’s Liberation Army Operational Concepts,” RAND Corporation, 2020, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA394-1/RAND_RRA394-1.pdf.

25『中華民国 110 年国防報告書』（台北：中華民国国防部 2021 年）41–44 頁。

そこで本稿は、最初に新たな領域といえども既に一般的になりつつあるサイバー領域と、まだその実体について議論が続いている認知領域の定義を確認し、そこで確認した概念に基づき、中国の公刊資料や諸外国の専門家による分析などを用い、中国のサイバー領域と認知領域におけるそれぞれの活動を整理していく。そのうえで、中国が全領域で繰り広げる「情報化戦争」の実例として台湾のケースを取り上げ、台湾に対する「認知領域における戦い」の特徴と効果を明らかにするとともに、伝統的な物理領域における破壊的なパワーの行使の有用性を発揮しつつも、兵士が血を流すことのないサイバー領域と認知領域での領域横断的な戦いを繰り広げることにより、敵と接触せずに目的の達成を目指す中国の「情報化戦争」の実態を読み解き、最後にその普遍性と特殊性を検討していきたい。

1.「サイバー領域」と「認知領域」の定義

本稿において「サイバー領域」とは、情報システムや情報通信ネットワーク等により構成され、様々な情報が流通するインターネットその他の仮想的なグローバル空間を指す[26]。このサイバー領域において、ネットワークや重要なシステムが何者かによって不正にアクセスされ、情報の窃取、流出、改ざん、無効化、破棄などの被害が多発している。そこで繰り広げられる不正行為が政府や生活インフラに深刻なダメージを与えるばかりでなく、社会を混乱させて人々に心理的な恐怖を与え、さらには人命の損失を招く事態まで発展することがあることは、セキュリティーアナリストのウィン・シュバルタウ（Winn Schwartau）が 2000 年に出版した『サイバーショック（Cybershock）』で警鐘を鳴らしており[27]、「サイバー攻撃」という用語が定着し、一定のコンセンサスが得られている。

「認知領域」で繰り広げられる戦いについては、十分にコンセンサスが得られる段階に至っていない。簡潔にポイントを示しているのは、ハーバード大学のオリバー・バックス（Oliver Backes）とアンドリュー・スワブ（Andrew Swab）による「対象者の考え方を変え、それによって対象者の行動様式を変えることを目的とした戦略」との定

26 サイバー空間の定義は多様だが、本稿では日本政府の「サイバーセキュリティ戦略」の定義を採用した（情報セキュリティ政策会議「サイバーセキュリティ戦略―世界を率先する強靭で活力あるサイバー空間を目指して―」高度情報通信ネットワーク社会推進戦略本部、2013 年 6 月 10 日、4 頁、https://www.nisc.go.jp/pdf/policy/kihon-s/cyber-security-senryaku-set.pdf）。

27 Winn Schwartau, *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption*, (New York: Thunder's Mouth Press, 2000).

義である[28]。近年では、ICT や AI 技術の飛躍的な発展に伴い、戦闘空間が物理的な範囲から「人間の認知[29]」を含む無形の空間に拡大し、認知領域をターゲットとした世論操作や情報操作が一国の政府の政策決定過程や世論形成過程に影響を及ぼしていることが指摘されている[30]。

他方、古くから非伝統的な安全保障の分野では、認知領域で戦いが繰り広げられていたと指摘されている。エール大学のサミュエル・ハンティントン（Samuel P. Huntington）は、1968 年に出版した『変化する社会における政治秩序（Political Order in Changing Societies)』のなかで、安定した伝統的社会にとって、外国の軍隊による侵略は主要な脅威ではなくなっており、むしろ外国思想の侵入こそが脅威であり、例えば印刷物などの活字は、戦車よりも速く、かつ深く侵入してくると論じている[31]。こうした古くからの人間の認知に対する脅威を踏まえ、NATO とジョンズ･ホプキンス大学の報告書では、「認知領域における戦い」について、①国民や政府の政策に影響を与え、②公的機関を不安定にすることを目的とした、外部勢力による世論の武器化と定義されている[32]。そして今日、サイバー領域で興隆するソーシャルメディアを通じて物理領域と認知領域が結びついている。

ソーシャルメディアは、情報の真偽を確かめる間もなく瞬時に拡散・共有する特性があるため、伝統的なプロパガンダと同じ内容であっても非常に小さなコストで大きな効果を得ることができる。とりわけインターネットや言論を統制する権威主義体制の国家とは対照的に、表現の自由を原則として開かれた社会の実現を目指す民主主義体制の国家は、ディスインフォメーション（disinformation；相手を傷つけるため意図的に拡散される偽りの情報）が拡散されやすく、それがリベラルな民主主義を脅かす存在になると警鐘が鳴らされている[33]。そこでロシアは、民主主義体制の国家における言論の自由に目を付け、その体制の根幹をなす「選挙」に照準を合わせ、サイバー領

28 Oliver Backes and Andrew Swab, *Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States*, (Cambridge: Belfer Center for Science and International Affairs, 2019), p. 8.

29「認知（cognition)」とは、もともと心理学で使われる用語であり、感覚や知覚、記憶など、生体が生得的または経験的に獲得した既存の情報に戻づいて、外界からの情報を選択的に取り入れ、それを処理して新しい情報を生体内に蓄積し、さらにはこれを利用して外界に適切な働きかけを行うための情報処理の過程をいう（酒井英明「認知」『世界大百科事典〔第 21 巻〕』（平凡社、1988 年）568 頁)。

30 桒原響子『「人間の認知」をめぐる介入戦略―複雑化する領域と手段、戦略的コミュニケーション強化のための一考察―』（東京大学先端科学技術研究センター、2021 年 7 月)。

31 Samuel P. Huntington, *Political Order in Changing Societies*, (New Haven: Yale University Press, 1968), p. 32.

32 Alonso Bernal, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla, *Cognitive Warfare: An Attack on Truth and Thought*, (Baltimore: NATO and Joshns Hopkins University, 2020), p. 3.

33 Freedom House, “The Rise of Digital Authoritarianism: Fake news, data collection and the challenge to democracy,” October 31, 2018, https://freedomhouse.org/article/rise-digital-authoritarianism-fake-news-data-collection-and-challenge-democracy.

域を通じて認知領域にアクセスすることで有権者の「認知」を操作し、自国の利益を有利に導く候補に利するようその投票行動を変えることを試み、それが成功したと評されている[34]。こうしたサイバー領域で拡散する情報が世論を左右し、政治にも影響を与えてきていることから、近年では「人間の認知」が国家の安全保障に重大な影響を及ぼす領域として注目を集めている。そして、この分野で先行しているロシアに続き、中国も政治や軍事に関する目的を達成するため、「認知領域における戦い」への取り組みを強化している。

2．中国の「サイバー領域」における活動

（1）人民解放軍におけるサイバー作戦能力の構築と発展

中国が「サイバー戦」に着目し、その能力構築に動き出す契機となったのは、1991 年の湾岸戦争における米国の圧倒的な勝利を観察したときのことである。中国は、米軍のネットワーク中心の戦い（Network-Centric Warfare: NCW）のコンセプトから学ぶ必要性を認め、その研究に着手した。その過程で人民解放軍は、米軍が情報技術に大きく依存していることを弱点の一つとして捉え、そのネットワークの重要なノード（節点）に対し、非対称な攻撃を行うことでその機能を麻痺させ、「弱者が強者を倒す」という独自の情報戦に関する方針を導き出した[35]。1999 年には、人民解放軍が軍内の人材を対象として、サイバー要員の養成を始めたが、その質・量ともに十分ではなかったため、情報産業から人材を探し出し、全国規模で「サイバー民兵」を組織した[36]。そして、陸、海、空、宇宙に続く第 5 の領域としてサイバー空間への関心が高まるなか、中国で「情報戦の父」と呼ばれる沈偉光は、敵のコンピューターシステムを破壊し、情報の受発信機構や金融、通信、エネルギー、交通など重要インフラのネットワークシステムを混乱させることで、敵の軍隊を戦闘不能に陥らせ、さらには国民からの信頼をも失墜させることができると主張した[37]。

2013 年 11 月の中国共産党第 18 期中央委員会第 3 回全体会議では、のちに「建国以来、最大の改革」と評価される国防・軍隊改革が発表された[38]。同会議において、インター

34 A Yang, “Reflexive Control and Cognitive Vulnerability in the 2016 U.S. Presidential Election,” *Journal of Information Warfare*, vol. 18, no. 3, Special Edition (Winter 2019), pp. 99–122.
35 John Costello and Joe McReynolds, *China’s Strategic Support Force: A Force for a New Era*, (Washington, D.C.: National Defense University Press, 2018), p. 2.
36 林穎佑「中国近期網路作為探討：従控制到攻擊」『台湾国際研究季刊』第 12 巻第 3 期（2016 年）59 頁。
37 沈偉光『信息邊疆：無影無形的第五邊疆』（北京：新華出版社、2003 年）36 頁。
38「中共中央関於全面深化改革若干重大問題的決定」『解放軍報』2013 年 11 月 16 日。

ネットが隆盛する時代に「サイバー空間」を管理する重要性が謳われた[39]。この時期、『解放軍報』の社説などで将来の戦争のニーズに応える「サイバー軍」の創設が語られることはあったものの、それが公式な方針として示されることはなかった。その方向性が明確になるのは、2015年9月3日の第二次世界大戦終結70周年を記念する式典において、習近平中央軍事委員会主席が人民解放軍の兵力を30万人削減する方針を示してからのことであった。次々と発表される軍事機構改革に関する内容の特徴として、兵力の量的削減のみならず、組織の質的転換が挙げられるが、そのハイライトの一つに、宇宙、サイバー、電子戦の任務を担う「戦略支援部隊」の新設が掲げられた。これにより、人民解放軍内に分散していたサイバー作戦部門が同部隊隷下のネットワークシステム部に概ね集約され、人民解放軍が行うサイバー領域における戦いが統一して運用される体制が整えられたのである[40]。

（2）国家安全部などによる「サイバー領域」での活動

近年、中国がインターネット上で、他国に対してネガティブな攻撃を仕掛けていることが指摘されている。例えば、早くも2009年12月中旬には、Googleが同社のGmailサービスに対して中国から入念に計画された標的型の攻撃を受けたことを発表している。中国のハッカーは、友人のアカウントを使ってメールやメッセージでURLを送りつけるほか、SNS上にURLを貼り付けた。そして、そのURLを不用意にクリックすると、悪意あるソフトウェアがパソコン内に保存されてしまい、ハッカーがいつでも侵入することができる[41]。2015年6月上旬には、中国のハッカーが米国政府の情報システムに侵入し、機密性の高いセキュリティー番号、セキュリティークリアランス一覧、業務申請書など、米国政府の現職および元職員とその配偶者の個人情報2,100万件以上がハッキングされた。その後、2年にわたる捜査の末、米国政府は中国国籍の男性を容疑者として逮捕している[42]。

最近では、2021年3月にマイクロソフト社のExchangeメールサーバーが攻撃を受け、データが漏洩している。ハッカーは、米国国内の大学、国防関連企業、法律事務所、感染症研究機関などセキュリティーが脆弱な情報システムに侵入し、それら機関

39「関於《中共中央関於全面深化改革若干重大問題的決定》的説明」『解放軍報』2013年11月16日。
40 John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, (Washington, D.C.: National Defense University Press, 2018), pp. 1–68.
41「《極光行動》発現疑中国黒客攻谷歌線索」VOA、2010年1月30日、https://www.voachinese.com/a/clues-of-chinese-hackers-were-behind-google-attack-20100129-83080367/460439.html。
42「涉竊美聯邦人事局資料 中国駭客被捕」公視新聞網、2017年8月25日、https://news.pts.org.tw/article/368944。

の機密情報を窃取した[43]。その事件を受け、7 月 19 日に米国、NATO 諸国、欧州連合（EU）、日本などは、中国政府が世界中で「無責任で悪質なサイバー活動」を行っており、その一環としてExchangeメールサーバーにサイバー攻撃をかけたハッカー集団を匿っていることを非難する声明を発表した。また、英国の国家サイバーセキュリティーセンターは、Exchange メールサーバーへの攻撃に関与したハッカー集団 Hafnium と関連があるとして中国国務院を名指しし、さらに、米国や欧州の防衛産業に対するハッキング行為を長年行ってきた APT 集団[44]のうち、APT31 と APT40 という 2 つのハッカーグループの背後に中国の国家安全部がいると名指で批判した[45]。これと同時期、米国司法省は 4 人の中国人を起訴した。4 人のうち 3 人は海南省国家安全庁の関係者、1 人は同庁が設立したフロント企業である「Hainan Xiandun（海南仙盾）」の一員であることが判明し、彼らは 2011 年から 2018 年にかけて、航空、国防、教育、政府、医療、バイオ製薬、海事などの分野に関する米国の企業、大学、政府のコンピューターシステムをハッキングした罪に問われた。米国側は、彼らが中国の国家安全部から報奨を得てハッキングを行ったと主張している[46]。

（3）「軍民融合」路線の基づく国家規模の「サイバー領域」における活動

習近平政権は、胡錦濤政権期に始まった「軍民融合による発展」の政策を継承し、さらにそれを推し進める方針を示している。2017 年 12 月 4 日に国務院から発表された国防科学技術工業の軍民融合に関する声明では、重点の一つにサイバー領域が挙げられている[47]。この「軍民融合」の枠組みで、中国のサイバー領域における活動が国家規模で発展していくことになった。ジョージタウン大学の安全保障・新興技術センターの調査によると、少なくとも 6 つの大学が、中国政府や人民解放軍の支援を受けた APT 集団と連携してサイバーセキュリティーに関する研究を行っており、最新の研究

43 Charlie Osborne, “Everything you need to know about the Microsoft Exchange Server hack,” ZDNET, April 19, 2021, https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/.

44 APT とは、サイバーセキュリティー企業のファイア・アイ社がサイバー攻撃集団を区別する際に用いるコードであり、Advanced Persistent Threat（高度で持続的な脅威）の略称である。

45 Christina Wilkie, “U.S., NATO and EU to blame China for cyberattack on Microsoft Exchange servers,” CNBC, July 19, 2021, https://www.cnbc.com/2021/07/19/nato-and-eu-launch-a-cyber-security-alliance-to-confront-chinese-cyberattacks.html; John Hudson and Ellen Nakashima, “U.S., allies accuse China of hacking Microsoft and condoning other cyberattacks,” *Washington Post*, July 19. 2021, https://www.washingtonpost.com/national-security/microsoft-hack-china-biden-nato/2021/07/19/a90ac7b4-e827-11eb-84a2-d93bc0b50294_story.html.

46「美司法部起訴四名中国黒客 国安化身「海南仙盾」被識破」自由亞洲電台、2021 年 7 月 19 日、https://www.rfa.org/cantonese/news/us-hackers-07192021091307.html。

47「国務院弁公庁関於推動国防科技工業軍民融合深度発展的意見（国弁発〔2017〕91 号）」中華人民共和国中央人民政府 HP、2017 年 12 月 4 日、http://www.gov.cn/zhengce/content/2017-12/04/content_5244373.htm。

成果が速やかに技術移転できる状態にあることが指摘されている[48]。また、2017年には、米国のサイバーセキュリティー企業によって、中国国家安全部の支援を受けたAPT41の活動が発見されている。2012年から活動を始めているAPT41は、中国本土の経済発展に資する情報の収集を専門とし、機械学習、自動運転、医用画像、半導体、プロセッサー、企業向けクラウドコンピューティングソフトウェアの研究開発に関連する企業などをターゲットにしている[49]。また、2020年5月にAPT41は、台湾の石油企業、プラスチック企業、半導体企業に対し、ランサムウェアを用いてシステムやデータを暗号化し、身代金を要求している[50]。

さらに中国は、民間のテクノロジー企業の名義でサイバー民兵を組織するほか、大手サイバーテクノロジー企業と協力してサイバー民兵を養成するための教室を運営している。 例えば、河北省の恒水南浩科技有限公司は、表向きは民間の技術会社だが、2006年以降、人民解放軍のサイバー民兵をリクルートしている。 また、2017年には安天ネットワーク科技公司という民間企業もサイバー民兵部隊を設立している。2019年9月には、広東省の中国科学院クラウドコンピューティング産業技術革新イノベーション・インキュベーションセンターが「サイバー民兵教室」を設立し、サイバー民兵の養成を始めている[51]。

2017年にドナルド・トランプ（Donald J. Trump）が米国大統領に就任した後、貿易摩擦を背景に米中間の緊張が高まると、中国から米国に対するサイバー攻撃が活発化した。 だが、米国の情報機関は、2018年になると人民解放軍によるハッキングのケースが無くなり、代わりに国家安全部の権限の下で活動するハッカーがそれを行うようになったことを発見した。米国の情報機関によると、現在、中国の経済活動に資するハッカー行為は、人民解放軍のサイバー作戦部門ではなく、中国の大手テクノロジー企業で働くエンジニアや、国家安全部門のフロント企業や請負業者によって柔軟に展開されている[52]。

こうして今日、中国のサイバー領域における活動は、「軍民融合」路線の下、人民解

48 Catalin Cimpanu, “Chinese universities connected to known APTs are conducting AI/ML cybersecurity research,” The Record, March 11, 2021, https://therecord.media/chinese-universities-connected-to-known-apts-are-conducting-ai-ml-cybersecurity-research/.

49 胡晴美「火眼点名中共駭客団体 APT41：間諜、商業犯罪双管斉下 14 個国家港台媒体都会被駭」『信傳媒』（2019年8月9日）https://www.cmmedia.com.tw/home/articles/16954。

50 黄彦棻「台美聯手防駭，追緝並起訴 APT41 中国網軍」iThome、2020年9月18日、https://www.ithome.com.tw/news/140054。

51 黄郁文「中共後備動員之研究：以網路民兵建設為例」財團法人國防安全研究院 HP、2020年9月30日、47–48頁、https://indsr.org.tw/uploads/Download/%E5%9C%8B%E9%98%B2%E6%83%85%E5%8B%A2%E7%89%B9%E5%88%8A-5.pdf。

52 Nicole Perlroth, “How China Transformed Into a Prime Cyber Threat to the U.S.,” *The New York Times*, July 20, 2021, https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html.

放軍のみならず、国家規模で多方面にわたって繰り広げられるようになっている。

３．中国の「認知領域」における活動

（1）広がりゆく「認知領域」における闘争の激化

中国において「認知領域」という言葉自体は新しいものであるが、その考え方は決して新しいものではなく、むしろ伝統的に人間の心の支配を重視してきた。例えば、毛沢東は 1938 年の著書『持久戦論』のなかで、日本との戦争に勝つためには「政治、経済、文化の進歩を促進するために努力し、労働者、農民、商人、学者などあらゆる階層の人々を動員し、敵の軍隊を解体してその兵士を獲得し、国際的な宣伝によって国際社会からの援助を勝ち取り、日本国民や他の被抑圧国の国民からの支持を獲得する。それ以外に優位に立つ方法はないだろう」と主張している [53]。

そして近年では、国際的に新興メディアが普及していく趨勢に伴い、中国は新旧メディアを包括した「認知領域」における活動へと移行している。中国は、偽情報を急速かつ大量に生成し、真偽を混在させたディスインフォメーションを拡散するプラットフォームとして、ソーシャルメディアの利用を重視している。中国の認知領域における戦い方は、新旧メディアをパッケージ化して展開することで、認知領域における戦いを優位に進めようとしている [54]。例えば、FacebookやLINE、TikTokなどのソーシャルメディアを利用し、個々のユーザーをターゲットにディスインフォメーションを発信している [55]。

このように中国が活動する「認知領域」が広がりゆくなか、国防大学国家安全学院の李明海は、かつて様々なメディアが戦場の様相を大衆に伝えるツールとして注目を集めたが、今はメディアそのものが主戦場になりつつあると指摘する。李は、戦争はもはや伝統的な物理領域での戦いにとどまらず、ソーシャルメディアにまで広がり、国際的な言論空間では銃弾を言葉に代えた戦いが繰り広げられ、それが認知領域における対立の主要な手段になっていると論ずる [56]。一方、国防科技大学の梁暁波は、「認知領域における戦い」について、現代の認知理論や科学の成果に基づき、インターネット、メディア、テキスト、写真、ビデオ、デジタル等の技術を利用し、人々の思考、

53 毛沢東『論持久戦』（1938 年 5 月）http://chinatide.net/xiachao/3-2.html。
54『中華民国 110 年国防報告書』44 頁。
55 李澄欣「“ 認知戦 ” 憂慮 vs 捍衛民主価値 台湾会徹底封殺抖音和 TikTok 嗎」BBC News 中文、2022 年 12 月 22 日、https://www.bbc.com/zhongwen/simp/chinese-news-64062953。
56 李明海「透視認知戦演変趨勢」『解放軍報』2022 年 9 月 29 日。

信念、価値観、アイデンティティーで主導権を得るために繰り広げられる伝統的なイデオロギー闘争の一形態だと主張する[57]。

中国など共産主義の国家は、その全体主義的な支配を維持するため、継続的な教育やプロパガンダを通じて人民の心に愛国心や党への忠誠心を植え付けようとする戦術を用いてきた。中国などが伝統的に行ってきた対内的に人民の支持を得て、対外的に敵の心を打ち砕き、国際宣伝に努めるという手法は、その活動の場が新興メディアに広がろうとも、今日の認知領域における戦いの基礎となっており、そこでの闘争は激しさを増している。

（2）人民解放軍などで活発化する「認知領域における戦い」の研究

中国では伝統的に人間の心の支配が重んじられてきたが、2000 年代に入って人民解放軍所属の研究者が将来の「情報化戦争」を論ずるなかで、物理領域やサイバー領域と並び、「認知領域」が注目され始めた[58]。2011 年に改訂された人民解放軍の軍事用語辞典『中国人民解放軍軍語（全本）』では、「情報化戦争」や「一体化統合作戦」構想の説明において、陸、海、空、宇宙、サイバー・電磁波空間に加え、「認知領域」が新たな作戦領域として示された[59]。こうして人民解放軍が伝統的に重んじてきた人間の認知に関する領域を新たな作戦領域として定義づけると、新たな戦場として公式に認められるようになった「認知領域」への関心が高まり、科学技術の発展と重なり合うように、それに関連する研究が活発化していった。2020 年 6 月には、戦略支援部隊の隷下にある情報工学大学学長の郭雲飛が、認知領域は大国間の軍事的対決の究極の領域になっていると指摘した。認知領域で行われる戦闘は、人間の脳に直接的に作用し、人間の感情、動機、判断、行動に影響を与えるばかりでなく、敵の思考や判断をもコントロールすることができる。 人間の認知の場である脳は、将来の戦争における主戦場になる可能性があり、脳をコントロールする能力が「認知領域における戦い」で勝敗を決める鍵となり、戦争における最高レベルのパワーになると説明した。さらに郭は、「戦わずして勝つ」という究極の目標を実現することができるのは、物理領域や情報領域での作戦ではなく、認知領域で行われる作戦だと主張する[60]。

また、呉中和や朱小寧といった中国の研究者は、『解放軍報』の社説において、中国は伝統的に偽情報を流布して敵を困惑させ、敵に間違った判断や決断をさせることに

57「梁暁波：認知域作戦是語源対抗新的主戦場」人民網、2022 年 5 月 17 日、http://military.people.com.cn/n1/2022/0517/c1011-32423539.html。
58 董子峰『信息化戦争形態論』（北京：解放軍出版社、2004 年）10–16 頁。
59 杉浦康之『中国安全保障レポート 2022』11–12 頁。
60 郭雲飛「認知域作戦進入制脳権争奪時代」『解放軍報』2020 年 6 月 2 日。

重点を置いてきたと主張する。彼らは、情報の不確実性によって人間の判断は容易に乱されると論じ、認知領域における戦いで鍵となるのは、敵が行う自軍の作戦行動に対する観察行動を混乱させ、正確な情報を得られなくすることで、状況判断の確実性を求める敵の心を根底から崩すことにあると説明する。そのうえで、敵からの観察を妨害するために着意する認知領域における戦いの手法として、偽装、妨害、欺瞞、沈黙など一般的な情報活動の要領に加えて、次の 4 つにも注意を払うべきであると訴える。1 つ目は、複雑な状況を作為することで「戦場の霧」を広げ、敵が自軍の状況を観察できないようにする。2 つ目は、敵の観察行動を妨害し、かつ、特定の目標に対する観察に集中させることで、真に重要な情報を獲得されないようにする。3 つ目は、虚偽を含むナラティブを形成することで、敵が観察した結果と客観的な事実に彼らの観察に矛盾を生じさせることで、混乱と事実誤認を招くようにする。4 つ目は、自軍の指揮官固有の意思決定スタイルを大切にし、さらに AI のアルゴリズムの活用など、敵に看破されない作戦行動を採ることが重要だと説明する [61]。

このように近年、人民解放軍では認知領域に関する研究や議論が繰り広げられているが、その新たな作戦領域にかかわる部門は、軍だけにとどまらない。中国国家インターネット情報弁公室（CAC）、中国共産党の中央宣伝部と中央統一戦線工作部、人民解放軍戦略支援部隊のほか、国務院台湾事務弁公室や民間のテクノロジー企業の下に編成されたサイバー民兵など「認知領域における戦い」に携わっている [62]。中国は、「戦わずして勝つ」という究極の目標の実現に向けて、その能力の構築に力を入れている。

4．中国が台湾に対して繰り広げる非接触型「情報化戦争」

（1）中国の台湾に対する「認知領域における戦い」の特徴と効果

台湾の 2021 年版『国防報告書』によると、台湾が直面する「認知領域における戦い」の脅威として、中国が政治的には、台湾の国際活動空間を圧迫することで、政治的要求を受け入れさせ、経済的には、経済･貿易上の優位性を利用して台湾企業や人々を引き込み、軍事的には、台湾海峡周辺の海・空域への侵入の頻度を高めるのと同時に、メディアやネットコミュニティーでそれを誇張することによって強要や抑止の効果を高め、心理面では、民衆の心を混乱させるとともに、軍人や民衆の抗戦の意思と

61 呉中和、朱小寧「基于作戦決策鏈破訳認知戦密碼」『解放軍報』2022 年 9 月 13 日。
62 黄文冰「軍民魚水情 結対共建暖民心」永泰新聞網、2017 年 1 月 17 日、http://www.fjytxww.com/2017-01/17/content_20557.htm.

自衛の決意を弱めさせ、世論の支配的地位を掌握しようとしていることが挙げられている[63]。かつて中国共産党は、中国国民党との内戦や朝鮮戦争において「人海戦術」で戦いを繰り広げてきたが、今日、認知領域で繰り広げられる戦いは、「情報による人海戦術」と表現することができる。台湾の蔡英文総統は、民主主義の社会でディスインフォメーションが拡散する速度は非常に速いため、中国が認知領域で繰り広げる戦いは、低コストで効率的な戦法であると述べ、それは台湾の存続に関わる最大の課題だと警鐘を鳴らしている[64]。

このように、中国が台湾に対する認知領域における戦いを強化している背景には、中国経済の低迷が指摘できる。中国の経済発展が好調だった頃は、台湾に対して様々な優遇措置や両岸交流の促進策など、ポジティブなプロパガンダで台湾の人々の心を惹きつけていたが、米中間の貿易摩擦や新型コロナウィルス感染症の世界規模での感染拡大も重なり、中国経済が大きく打撃を受けると、中国はディスインフォメーションを流布することで台湾社会の分断を企て、プロパガンダの性質もネガティブなものへと変化している[65]。

こうした中国の認知領域における戦いの経路を分析した台湾の専門家は、大きく「金銭」「人」「情報」の 3 ルートに分けて説明する。まず、「金銭」ルートは、台湾の住民、ライブストリーマー（動画配信者）、広告宣伝会社などに報酬を支払い、主に台湾の若者をターゲットに親中世論を広めることを狙っている。2000 年の総統選挙前には、台湾の人気ユーチューバー TOP10 のうち、6 名が中国の金銭的な援助を受けて親中メッセージを流していた。「人」ルートについては、伝統的な統一戦線工作の方式の一つで、中国は台湾の地方の村長や学校に通う若者などを協力者として獲得し、彼らを通じで宣伝活動を展開する。出稼ぎで中国大陸に行く台湾の住民も、そのターゲットになりやすい。最後の「情報」ルートとは、新聞、テレビ、ラジオなどの伝統的なメディアに宣伝用の広告を掲載するほか、中国共産党の「赤」い思想に染まっていないものの、中国に対して良好なイメージを抱く「ピンク」がかった若者が、特に中国からの指示を受けることなく、不特定多数の台湾住民に向けて自発的に中国の利する情報を発信

63『中華民国 110 年国防報告書』44 頁。
64「蔡英文：資訊戰與認知作戰是台湾生存最大挑戰」中央通訊社、2022 年 8 月 10 日、https://www.cna.com.tw/news/aipl/202208100290.aspx。
65 Tzu-Chieh Hung and Tzu-Wei Hung, “How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars,” *Journal of Global Security Studies*, vol. 7, no. 4 (December 2022), pp. 11–13, https://doi.org/10.1093/jogss/ogac016.

するように仕向けるものである[66]。

このように中国が台湾に仕掛けてくる認知領域における戦いにおいて、そこで流布するディスインフォメーションを分析すると、①中国の台湾侵攻に対する防衛作戦準備、②蔡英文総統の権威、③台湾と欧米諸国との関係、という 3 つの特徴が際立って見えてくる。1 つ目の防衛作戦準備については、「台湾の政府は侵攻に対する準備ができていない」「台湾の人々は、いくら抵抗しても無駄だと考えている」といった批判が拡散されている。2 つ目として、ウクライナのヴォロディミル・ゼレンスキー（Volodymyr O. Zelenskyy）大統領がメディアを通じて国際社会に訴え、国際社会からの支持を集めているように、中国が台湾に侵攻した際、蔡英文が同じように象徴的な存在になることを妨げるため、その権威を失墜させようとしている。3 つ目は、台湾の人々に欧米に対する不信感を植え付けようとしている。ウクライナに対する米国の支援が限定的であることを見て、台湾の人々の間で「米国は台湾を見捨てるのではないか」といった不安が広がっている。こうしたディスインフォメーションが拡散する背景には、欧米や日本のメディアが中国のコンテンツファームやフェイクニュースサイトに飛びつき、それを引用し、さらに人々の注目を集めるように潤色して報じていることが挙げられる。中国側から発信されるディスインフォメーションの影響を直接的に受けるばかりでなく、欧米メディアから発信されるニュースが台湾で「疑米論」が広がる要因となっている[67]。

このような中国が台湾に対して進めている認知領域における戦いは、短期的な目標の達成を狙うものが多くを占めているが、長期的に繰り返すことで文化的な浸透を図ることへと繋がっている。例えば、言語である。中国と台湾では、同じ中国語でも台湾は伝統的な繁体字を用い、中国は簡略化した簡体字を用い、その違いを一目で見分けることが可能である。また、同じ意味を指す言葉でも単語が異なる場合があり、日本で「タクシー」を意味する単語が台湾では「計程車」、中国では「出租車」と表記される。近年、動画サービス Tik Tok を見る若者が増えているが、その配信で使われる中国の文字や単語が台湾でも広まり、中国と台湾で全く同じ文字や単語が使われるようになると、ディスインフォメーションの判別も難しくなる。中国と台湾は文化などの面で共通する歴史を有するがゆえに、人間の心の中、すなわち人間の「認知領域」

66「専訪：中国瞄準台湾年軽人進行反美日認知戦」Deutsche Welle 中文網、2021 年 11 月 10 日、https://www.dw.com/zh/%E4%B8%93%E8%AE%BF%E4%B8%AD%E5%9B%BD%E7%9E%84%E5%87%86%E5%8F%B0%E6%B9%BE%E5%B9%B4%E8%BD%BB%E4%BA%BA%E8%BF%9B%E8%A1%8C%E5%8F%8D%E7%BE%8E%E6%97%A5%E8%AE%A4%E7%9F%A5%E6%88%98/a-59764718。

67 A.A. Bastian, “China Is Stepping Up Its Information War on Taiwan,” *Foreign Policy*, August 2, 2022, https://foreignpolicy.com/2022/08/02/china-pelosi-taiwan-information/; 沈伯洋「中国認知領域作戦模型初探：以 2020 台湾選挙為例」『遠景基金会季刊』第 22 巻第 1 期（2021 年 1 月）30–47 頁。

で激しい争いが繰り広げられているのである。

（2）中国の台湾に対する領域横断的な非接触型「情報化戦争」の事例分析

中国が台湾に侵攻する際、第一波はミサイル攻撃だと言われているが、物理領域での戦いが始まる前に、目に見えないサイバー領域や認知領域において戦いが始まると指摘されている。しかし、1949 年の分断以来、台湾海峡に「平時」は無く、常に臨戦状態にあり、その「グレーゾーン」で繰り広げるサイバー領域や認知領域の戦いにおいて中国は、必要により物理領域のアセットを組み合わせ、「戦わずして人の兵を屈する」ことを試みている。それは、実際に軍事力を行使することなく、相手に軍事力を誇示することでその意思に従わせようとする「強要」の効果を利用するものであり[68]、その最たる事例が、2022 年 8 月にナンシー・ペロシ（Nancy P. Pelosi）米下院議長が台湾を電撃訪問した際、台湾社会が見舞われたサイバー攻撃であり、ペロシ離台後の人民解放軍による軍事演習であった。

8 月 2 日 22 時過ぎ、アジア歴訪中のペロシは、中国が「報復の可能性がある」と警告するなか、台北に到着した。その時、既に「サイバー領域における戦い」は激しさを増していた。8 月 3 日、台湾の政府は、2 日に行政機関が受けたサイバー攻撃のデータ量の合計が過去最も多かった日の 23 倍に上る 1 万 5,000 ギガバイトに達したことを発表した[69]。ペロシが蔡英文ら要人と会談を繰り返した 3 日には、台湾の大手コンビニチェーン・セブンイレブンの複数店舗で電光掲示板に「ペロシは台湾から出ていけ」と、台湾鉄道各駅の電光掲示板に「ペロシを歓迎した者は、人民の審判を受ける」と中国大陸で用いられる簡体字で表示された[70]。そしてペロシが台湾を離れた翌日の 4 日、外交部報道官が記者会見において、外交部公式サイトに中国やロシアの IP アドレスから 1 分間に 850 万回のアクセスがあったため、サーバーがダウンしてアクセスが不能になったことを発表している[71]。

ペロシ訪台を受け、中国は台湾を取り囲むように 6 か所のエリアを設定し、「重要軍事演習」を行うことを発表した[72]。ペロシらが離台した 4 日以降、人民解放軍は台湾周辺で 11 発のミサイル発射を行い、一部のミサイルは台湾上空を超えて台湾東部海域

68 Thomas C. Schelling, *Arms and Influence*, New Haven: Yale University Press, 1966, pp. 69–91.
69「因応今日政経情勢 政院：公私協力共同合作 防止外力不当侵擾 確保政府及社会運作如常」行政院 HP、2022 年 8 月 3 日、https://www.ey.gov.tw/Page/9277F759E41CCD91/7b9ee9dd-0283-4800-91ef-2781b2ba0e27。
70「広告蛍幕単日収視万 900 人次 統一超商遭駭客鎖定」自由時報 HP、2022 年 8 月 4 日、https://news.ltn.com.tw/news/politics/paper/1532483。
71「有関網路流伝有心人士截取美国聯邦衆院議長裴洛西受訪影片事，外交部回應如下」中華民国外交部 HP、2022 年 8 月 11 日、https://www.mofa.gov.tw/News_Content.aspx?n=99&s=98255。
72「我軍在台島周辺海空域成功挙行実戦化総合演訓」『解放軍報』2022 年 8 月 5 日。

に着弾したと報じられた[73]。また、空軍機が台湾海峡の中間線を超えて飛行する事例が激増し、国防部は5日までの統計で延べ49機が中間線を越えたと報じた[74]。この演習は、その公表したエリアを見て 1995 年から 1996 年の「第 3 次台湾海峡危機」以来の危機が訪れると予想する声が上がったが、8 月 10 日には軍事演習の全行程が終了したことが発表された[75]。

こうした軍事的な「強要」とサイバー攻撃に重なり合わせるように、中国は「認知領域における戦い」を展開した。台湾の国防部は 8 月 8 日に記者会見を開き、人民解放軍が台湾周辺で軍事演習を行って圧力を加えるのと同時に、総統府や国防部など政府機関の公式サイトに対してサイバー攻撃をしたことを明らかにした。また、軍事演習が始まる前から 8 月 8 日までの間に、272 件のディスインフォメーションが拡散され、その内容は、①台湾を武力で統一する雰囲気を醸成する、②台湾の政府の威信を損なう、③台湾の軍隊と民衆の士気を乱す、の大きく 3 つに分類できると公表された[76]。

このほか、軍事演習の発表前から Twitter や Weibo（中国版 Twitter）上に、「中国は福建省で武器を大量に増産している」などの書き込みや、台湾の対岸で戦車が走行している画像などが拡散されていた。こうした投稿の多くは流言であり、画像なども過去の写真や動画を合成したものであることが台湾ファクトチェックセンターから報告されている。これが中国や台湾のソーシャルメディアで流布している限りでは、台湾の人々はディスインフォメーションとして目に留めないかもしれないが、欧米メディアがそれを吟味することなく取り上げることでグローバル規模に拡散し、それを信憑性が高い記事として台湾の主要メディアが引用することで、台湾の人々の感情や認知に影響を及ぼすことになる[77]。

さらに軍事演習の終了直前、中国は「台湾問題と新時代の中国統一事業」と題する白書を発表し、祖国統一に向けた指針を示した。中国は 1993 年 8 月に「台湾問題と中国の統一」、2000 年 2 月に「一つの中国原則と台湾問題」という白書を発表しており、台湾問題に関する白書は今回で 3 回目となる。新たな白書では、従来の路線と変わらず「平和的統一と『一国二制度』は、台湾問題を解決するための基本的なアプローチ

73「共軍 8 月飛弾越台湾上空 邱国正：跨越領空算第一撃」中央通訊社、2022 年 10 月 14 日、https://www.cna.com.tw/news/aipl/202210140199.aspx.
74「共機 49 架次擾台歴年第 2 多 24 架次蘇愷 30 逾越中線」中央通訊社、2022 年 8 月 5 日、https://www.cna.com.tw/news/aipl/202208050392.aspx.
75「東部戦区在台島周辺海空域組織的聯合軍事行動成功完成各項任務」『解放軍報』2022 年 8 月 11 日。
76「中共軍演也打「認知作戦」国防部：本月已 272 則争議訊息」自由時報 HP、2022 年 8 月 8 日、https://news.ltn.com.tw/news/politics/breakingnews/4018471。
77「看穿中国心戦四大伎倆 打造資訊防禦力」台湾事実査核中心 HP、2022 年 8 月 16 日、https://tfc-taiwan.org.tw/articles/8033。

であり、民族統一を実現するための最善の方法である」と謳われている[78]。一方で、前回までの白書で示されていた「統一後の台湾に軍隊や行政官を駐留させない」という記述がなくなっており、大きく方針が転換されている。軍事演習とサイバー攻撃が繰り広げられるなかで発表されたこの白書についても、「認知領域における戦い」の一環と評することができる。それには、甘い言葉で「懐柔」を図ろうとするばかりでなく、「威嚇」のメッセージが隠されていた。

中国が台湾の対岸で軍事演習を行うことに台湾の人々は「慣れ」てしまい[79]、それはもはや「強要」の効果を失いつつあった。中国は、ペロシ訪台前後に繰り広げた一連の軍事演習やサイバー攻撃に「認知領域の戦い」を組み合わせる形で、その「強要」の効果を取り戻すことを試みたのである。中国がペロシ訪台を成果として掲げようとする台湾の政権に加えた圧力は、中国の領域横断的な非接触型「情報化戦争」の一形態だったと言えよう。

この一連の軍事演習やサイバー攻撃について、日本や欧米などのメディアは「第四次台湾海峡危機」と呼び、その動向を注視した[80]。しかし、現地・台湾の人々は、圧倒的多数がその軍事演習を「怖くなかった」と語り、中国が軍事演習を行うなかでも普通の生活を送っていた。台湾社会がパニックになっていたら、それこそ中国の思うつぼであったが、威嚇によって屈服させようとする中国の思惑は台湾に通じなかったのである[81]。

おわりに

本稿では、サイバー領域と認知領域の定義を確認したのち、そこでの中国の活動を整理したうえで、それに物理領域を加えた全ての領域で横断的に繰り広げられる非接触型の「情報化戦争」について、台湾を事例にその実態を理解する手がかりを考察し

78「台湾問題與新時代中国統一事業（2022 年 8 月）」『人民日報』2022 年 8 月 11 日。

79 朝日新聞のインタビューに応じた台湾の王尊彦氏（国防安全研究院）は、中国が 2022 年 8 月に軍事演習を行った際、台湾社会では普段と変わらない生活が続き、市民は落ち着いていた、市民は中国の圧力に慣れている、と述べている（「ペロシ氏訪台の批判は筋違い 台湾の日本研究者が語る日台関係」『朝日新聞』2022 年 8 月 15 日、https://www.asahi.com/articles/ASQ8D6KMXQ8DUHBI02P.html）。

80 Ankit Panda and Catherine Putz, “A Fourth Taiwan Strait Crisis or an Inflection Point for the Status Quo?: What do the events of early August 2022 in the Taiwan Strait portend for the future of the Asia-Pacific?,” The Diplomat, August 17, 2022, https://thediplomat.com/2022/08/a-fourth-taiwan-strait-crisis-or-an-inflection-point-for-the-status-quo/.

81 小笠原欣幸「ペロシの台湾訪問が中国を「やりにくく」させた訳―軍事演習を正当化する口実を与えたのはマイナス―」東洋経済 ONLINE、2022 年 10 月 3 日、https://toyokeizai.net/articles/-/622584.

てきた。

孫子が究極的な兵法として「戦わずして人の兵を屈する」と説いているように、中国は物理領域において「戦わずして勝つ」という究極の目標の実現に向け、2015 年の『戦略学』で記述された「敵と接触することのない作戦」の能力構築に力を入れている。それを実現するための重要な空間が、本稿でその定義やそこでの活動を整理してきた「サイバー領域」であり、「認知領域」である。中国は、サイバー領域において、対象とする国のシステムやネットワークを麻痺させるとともに、その重要なデータの窃取を試み、認知領域では、対象とする国の市民の心を捉え、その解釈や理解に影響を与えることに重点を置いている。

今日、仮想的なグローバル空間で繰り広げられる「サイバー領域における戦い」、とりわけ情報の窃取、改ざんなどの被害をもたらす「サイバー攻撃」については、それを担う機関や手法は各々の国で異なれど、一定のコンセンサスが得られている。一方、「認知領域における戦い」については、第 1 節で「対象者の考え方を変え、それによって対象者の行動様式を変えることを目的とした戦略」との定義を提示しているが、十分にコンセンサスが得られる段階に至っていない。そこで本稿では、台湾海峡を挟んで対峙する中国と台湾を事例として取り上げ、中国の台湾に対する「認知領域における戦い」について考察した。

その特徴として、人々の心の中へと浸透していく経路やそこで流布するディスインフォメーションの内容などを挙げたが、他の国とは異なる大きな特徴として、共通の言語を通じて対象者の心の中へと浸透できることを指摘した。中国と台湾はともに中国語を公用語としており、そこで繰り広げられる「認知領域における戦い」の手法は、中華圏に限定された特殊なケースであるかもしれない。しかし、そこで使われている文字や単語がそれぞれ異なることから、その違いを一目で見分けることができ、それがディスインフォメーションの拡散を防ぐ要因の一つになっていることを指摘した。このことは、日本でも受信したメールのフォントや文法が不自然であれば、詐欺メールやスパムメールだと判断していることなどと共通している。つまり、「人間の認知」を操作しようとするのであれば、主に対象者の視覚を通じて情報を得なければならず、そのためには言語は極めて重要なツールであり、文字や文法などの正確性がその成否を左右する要素になっていると言えよう。

反対に、「認知領域における戦い」を仕掛ける側としては、対象者の言語特性のみならず、その習慣など文化的背景まで理解を深めなければ、期待する効果を得ることは難しい。この問題を克服するためには、一つに対象とする国から協力者を獲得する手

段が考えられるが、それでは明らかに非効率である。それを最も効率的に克服することができるのは、AI 技術の活用なのではなかろうか。最先端の AI 技術で言語や文化の壁を克服し、認知領域での優勢を獲得することで、物理領域と情報領域における優勢をより確保することへと繋がり、それが領域横断的な非接触型「情報化戦争」の到達点になることであろう。そしてその先には、中国が目指す「智能化戦争」の青写真が描かれている。

2022 年 8 月のペロシ訪台前後、中国は台湾に対して領域横断的な非接触型「情報化戦争」を仕掛けたのだが、それは失敗に終わった。現時点で中国が台湾に対して繰り広げる領域横断的な非接触型「情報化戦争」の形態を見る限り、平素より対策を講じ、過剰に反応しなければ、その効果を無効化もしくは低減可能であることを台湾は証明した。また、2014 年から始まったロシアとウクライナの間の紛争を見ても、サイバー領域や認知領域での戦いが戦争全体の帰趨を左右したとは言い難く、むしろその限界が示され、それだけでは戦争に勝てないことが証明されている。だが、かつて「人海戦術」で自らの人民の命を顧みなかった中国でも、今では少子高齢化の影響を受け、軍隊は募集難に苦しみ、「兵士の命」の重要性が増している[82]。それゆえに中国は、「戦わずして勝つ」という究極の目標を目指し、領域横断的な非接触型「情報化戦争」の能力を構築に努力していくであろう。

中国にとって台湾は、祖国統一のために奪還すべき領土の一部であることは変わらない。そして今日、その台湾は、中国が領域横断的な非接触型「情報化戦争」の能力を国家総動員で構築していくための「試験場」になっている。

（中共軍事事務研究所）
（防衛研究所）

82 五十嵐隆幸「中共武装力量的人力資源問題：面臨少子化及高齢化時代的中共解放軍」『中共解放軍研究学術論文集』第 3 期（2021 年 12 月）189–220 頁。

〔付記〕本稿は、日本台湾交流協会 2022 年度「共同研究助成事業（人文・社会科学分野）」の助成を受けて行った研究成果の一部である。