民主主義国家の「サイバー軍」による攻勢的サイバー作戦能力の整備と運用
──米軍とオランダ軍における「二重の統合」の過程に着目した比較事例研究──

瀬戸　崇志

＜要旨＞

本稿では、「サイバー軍」とも称される軍事組織のサイバー戦力（MCF：military cyber forces）と攻勢的サイバー作戦能力（OCC：offensive cyber capabilities）をめぐる学術研究の検討を踏まえ、既存のインテリジェンス機関と別個に存在するMCFが、OCCの整備/運用で果たす特有の機能の把握を試みた。本稿は民主主義国のMCFがOCCの即応性確保のため、（1）軍事作戦への能力の「統合（integration）」と（2）軍の作戦部門とインテリジェンス機関の能力の「統合（fusion）」からなる「二重の統合」を促すとの仮説に従い、米蘭2か国のMCFの比較事例研究を行った。事例研究の結論は米蘭のMCFの「二重の統合」の機能を支持しつつ、MCFによるOCCの整備/運用の在り方が、各国の戦略目標、国内政治過程、法制度等による内在的制約に拘束されることも示した。

はじめに

2021年9月に閣議決定された日本政府の「サイバーセキュリティ戦略」は、近年のサイバー空間をめぐる国家安全保障上の情勢認識の記述のなかで、「中国・ロシア・北朝鮮において、軍をはじめとする各種機関のサイバー能力の構築・増強（後略）」や「同盟国である米国や基本的価値観を共有する同志国においても、サイバー脅威に対応するため、サイバー軍の能力構築が加速される（後略）」（下線部筆者）と言及した[1]。

前段の「サイバー軍」とは、各国の実力組織である軍隊（armed forces）または国防省等の文官組織を含む軍事組織の隷下にある「サイバー部隊（cyber force）」や「サイバーコマンド（cyber command）」と呼称される機構の訳語とみられる。特に2010年代以降、こうしたサイバー空間の課題に対処する軍事組織内の機構の新編は世界的

1　内閣サイバーセキュリティセンター「サイバーセキュリティ戦略」2021年9月28日、29頁、https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf。

にも拡散傾向にあり、欧米諸国の安全保障研究でも大きな関心を集めてきた。かような軍事組織内の機構を「軍事組織のサイバー戦力（MCF：military cyber forces）」、これを観察対象とする学術研究を MCF 研究と総称した場合、MCF 研究は、サイバー空間のガバナンスの主体としての軍事組織の特殊性に着目し、MCF とその他の政府機関、民間企業や犯罪集団を含む非国家主体の異同や相互の関係性の実証と理論構築を目指してきた。

それにもかかわらず従来の日本国内のサイバー保障研究では、国家安全保障を担う政府機としては通信情報（SIGINT：signal intelligence ）を司るインテリジェンス機関（intelligence services）[2]（以下:INTEL）の機能は着目されてきたが、これに対して近年における MCF 研究の発展には殆ど関心が払われてこなかった。以上を背景として、本稿は次の 2 点を目的とする。第 1 に、軍事力の「整備」と「運用」（以下：整備 / 運用）[3] ならびに「即応性（即応態勢:readiness）[4]」の概念を補助線に、NATO 加盟国を中心とした民主主義国の MCF による攻勢的サイバー作戦能力（OCC：offensive cyber capabilities）の整備 / 運用をめぐる先行研究の検討を行う。

第 2 に、本稿では民主主義国の MCF が、先行して OCC を整備 / 運用してきた既存の INTEL との関係のなかで、能力整備 / 運用で果たす独自の機能を明らかにする。この点を研究上の問いとして表現すれば、「各国で、既存の INTEL が MCF に先行して OCC の整備 / 運用に関与してきた歴史的経緯にもかかわらず、なぜ一部の民主主義国では新編された MCF を軸に OCC の整備 / 運用が進められていくのか」と表現できる。この問いに対し、本稿は近年の民主主義国の MCF が「軍種間の統合（joint）」とは異なる２つの意味での統合を促すことで OCC と呼ばれる軍事力の即応性を確保する機能を備え、この能力の整備 / 運用の軍事的合理性を追求するために MCF は編制されるとの仮説（以下:「二重の統合仮説」）を置く。本稿は、この「二重の統合仮説」を、2010 年代以降の OCC の整備 / 運用を任務に掲げた米蘭の 2 か国の MCF の比較

2　例えば次を参照。土屋大洋「サイバーセキュリティとインテリジェンス機関―米英における技術変化のインパクト」『国際政治』第 179 号（2015 年 2 月）44–56 頁。

3　本稿で「運用」とは、「軍事組織が保持する能力（兵力：capabilities）を実際の任務に投入して所期の目標を達成する取組」であり、「整備」とは「運用の時間軸の前後で、軍事力の機能の造成と維持を行う取組」を指す。こうした軍事組織の一般的な機能については、次を参照。高橋杉雄「基盤的防衛力構想からの脱却－ミッション志向型防衛力の追求－」『国際安全保障』第 44 巻第 3 号（2016 年）56–57 頁；千々和泰明「戦後日本の安全保障政策に関する分析枠組みとしての『防衛力整備／運用』―『限定小規模侵略独力対処』概念を手がかりに」『年報政治学』65 巻 1 号（2014 年）332–351 頁。

4　「即応性」とは、軍事力の状態を示し、特定の能力（兵力）を任意の地域・時期・期間で運用し、付与した任務を完遂しうる状態を指す。軍事組織による能力「整備」の機能とは、究極的には能力の即応性の確保・維持にあり、そのために部隊新編やドクトリン形成、装備品の調達・配備、要員の訓練・演習等の多様な行政管理機能を担う。即応性の概念やその確保・維持の論点は次を参照。U.S. Library of Congress, Congressional Research Service, *The Fundamentals of Military Readiness*, by G. James Herrera, R46559 (October 2020).

事例研究で検証する。

以下、本稿は次の構成を取る。第 1 節では、先行研究を踏まえた MCF の定義とあわせて、MCF をめぐる学術研究の体系に連なる本稿が扱う問題の所在とアプローチを確認する。第 2 節では、第 1 節で設定した問題の所在に沿って、MCF による OCC の整備 / 運用をめぐる主要な先行研究を横断的に整理検討した後に、本稿が掲げる「二重の統合仮説」の操作化を行う。第 3 節では、第 2 節の内容を踏まえた「二重の統合仮説」を検証する比較事例研究の分析枠組を明らかにしたうえで、第 4 節と第 5 節では、第 3 節までに示した仮説と分析枠組に沿って、米蘭 2 か国の MCF の新編 / 改編の経緯と OCC の整備 / 運用への関与の動向の観察を通じ、本稿の仮説の妥当性を検証する。「おわりに」では、事例研究の結果を要約し、その含意と将来の研究課題に触れて結びと代える。

1．MCF 研究として本稿が扱う問題の所在とアプローチ

（1）本稿における軍事組織のサイバー戦力（MCF）の定義

本稿はピレ・ペルニク（Piret Pernik）やジョン・ブレッシング（John Blessing）による先行研究の成果に依拠し、MCF を「各国の正規の軍事組織の指揮命令系統下にある機構であり、かつ（1）防勢的サイバー作戦（DCO：defensive cyber operations）、（2）攻勢的サイバー作戦（OCO：offensive cyber operations）、（3）サイバー空間を通じた情報収集・警戒監視・偵察活動（C-ISR：Cyber Intelligence, Surveillance and Reconnaissance）等に分類されるサイバー作戦（CO：cyber operations）[5] のうち、いずれか 1 つ以上の CO の直接的な遂行権限を付与されたもの」と定義する [6]。

この定義は MCF を、各国の軍事組織の指揮命令系統下に置かれ CO の遂行（運用）に責任を負う機構と捉え、独立の軍種（services）から、既存軍種要員から編制され

5　CO は米軍や NATO のドクトリン上では「サイバー空間作戦（cyberspace operations）」とも表記されうるが、含意の相違はないため、本稿では「サイバー作戦」の記載で統一する。DCO、OCO、C-ISR の定義と射程は、次を参照。Piret Pernik, *Preparing for Cyber Conflict: Case Studies of Cyber Command*, Report (Tallinn: International Centre for Defence and Security, 2018), pp. 2–3.

6　本稿では全軍種からなる統合的なサイバーコマンドのみならず、下位の軍種単位での司令部・部隊等も検討対象に含む点から、ブレッシングの表記に Military との形容詞を付した MCF との表記を用いる。両名の先行研究上の定義は、次を参照。Piret Pernik, “National Cyber Commands,” in *Routledge Handbook of International Cybersecurity*, ed. Eneken Tikk and Mika Kerttunen, 1st Edition (London: Routledge, 2020), pp. 187–188; Jason Blessing, “The Global Spread of Cyber Forces, 2000–2018,” in *13th International Conference on Cyber Conflict: Going Viral*, ed. T. Jančárková et al., (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence [hereafter NATO CCDCOE], May 2021), pp. 235–240.

るコマンド（commands）、部局（brunches）、部隊（units）まで多様な規模や編制形態を想定する。この定義は予備役部門や民間の請負業者等、人材育成や技術提供の面で能力整備に寄与しつつも CO の遂行権限を持たない主体、軍事組織の公式の指揮系統外で動員されるサイバー犯罪集団等の非国家主体、そして軍事組織とは異なる指揮系統に服す文民系統の INTEL（Civ-INTEL: civilian intelligence services）を除外する[7]。

（2）問題の所在と本稿の射程：国家による OCC の組織的統合をめぐる実証研究

本稿は、近年の MCF と OCC をめぐる学術研究や実務の論点の一部のみを扱うものであり、具体的には「国家（政府）の軍事組織としての MCF」による「（軍事力の一部としての）OCC の整備 / 運用の課題」に射程を絞って研究を進める[8]。このスコープの設定の理由には、既存の先行研究の動向を踏まえた以下の 2 点の背景を挙げることができる。

第 1 に、近年の MCF 研究は、NATO 加盟国を中心とする各国の MCF による OCC の整備 / 運用の動向と相互作用しつつ発展を遂げてきたからである[9]。マックス・スミーツ（Max Smeets）を筆頭に、近年の MCF と OCC をめぐる先行研究の問題意識を端的に要約すれば「個人や犯罪集団による単発のサイバー攻撃の可否と、国家機関が政策目標の達成手段として運用可能な即応性を備えたサイバー攻撃の展開能力は異なる」と表現できる[10]。こうした近年の先行研究は、この点を各国政府の機密指定解除済文書、民間企業のデータ、官民の実務家達の証言等を含む各種公刊資料から実証し、2010 年代前半頃に形成されたサイバー攻撃の戦略的価値をめぐる議論の修正を迫ってきた。こうした先行研究の整理は、それ自体が日本国内の MCF/OCC をめぐる学術論争の空白を埋める意義を持つ。

7　予備役部門や Civ-INTEL の除外の背景は次を参照。Ibid., p. 236; Sergei Boeke and Dennis Broeders, “The Demilitarisation of Cyber Conflict,” *Survival*, vol. 60, no. 6 (November 2018), pp. 75–79.

8　厳密には OCC の概念は必ずしも国家の能力のみを指す訳ではない。ただし本文で触れる通り、政府機関と非国家主体では、即応性の確保･維持の要請をはじめ、必要とされる能力の水準や整備 / 運用の制約条件が異なる。したがって、本稿は MCF という政府機関が扱う OCC に焦点を絞る形での検討を進める。

9　代表例は次を参照。Max Smeets, “NATO Members’ Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis,” in *11th International Conference on Cyber Conflict: Silent Battle*, ed. T. Minárik et al. (Tallinn: NATOCCDCOE, May 2019), pp. 163–178; Jeppe T. Jacobsen, “Cyber Offense in NATO: Challenges and Opportunities,” *International Affairs*, vol. 97, no. 3 (May 2021), pp. 703–720.

10 こうした議論は特に次を参照。Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (London: Hurst Publishers, 2022), pp. 33–49; Austin Long, “A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning,” in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Washington DC: Brookings Institution Press, 2018), pp. 105–132.

第 2 には、本稿の「二重の統合仮説」に沿った比較事例研究は、MCF 研究のなかで OCC の組織的統合[11]と呼ばれる課題をめぐる論争の発展にも貢献しうる。近年の先行研究は、一定の OCC の整備 / 運用に際して、本稿の「第 2 の統合」の要請が強く働く点を示唆してきたが、トビアス・リーベトラウ（Tobias Liebetrau）による近年の例外[12]を除くと、各国の政策過程での「第 2 の統合」のプロセスを過程追跡した実証研究は乏しい。また先行研究では、能力の整備 / 運用の過程を既存の INTEL に強く依存する OCC を念頭に、MCF による OCC の整備 / 運用の所要を捉えてきた。しかし、そこでは後述する既存の INTEL への依存度が異なる OCC と、その整備 / 運用を目指す MCF の位置づけは定かではない。以上を踏まえ第 2 節では、本稿の「二重の統合仮説」を軸とする分析枠組の構築に向けて、MCF と OCC をめぐる先行研究が示してきた中核概念や前提の整理検討を行う。そして第 3 節では米蘭両国の比較を通じ、上記先行研究の課題の克服を試みる。

2．MCF/OCC 研究の横断的検討を通じた「二重の統合仮説」の構築

（1）攻勢的サイバー作戦（OCO）と攻勢的サイバー作戦能力（OCC）

前項の問題設定と主要な先行研究を敷衍する形で、本稿では OCO と OCC を、それぞれ MCF を含む国家機関が司る作戦と能力として次の通り定義する。まず OCO は「サイバー空間を通じて、第 3 者のネットワーク、システム、データ等の標的の情報資産の利用の拒否（deny）、一時的な機能妨害（disrupt）または減損（degrade）、あるいは回復不可能な完全破壊（destroy）といった軍事的効果（effect）（頭文字を取って「4D」とも呼ばれる）をもたらす作戦行動」である[13]。OCC は、この OCO の遂行に必要となる「攻撃ツールや攻撃インフラ等の技術的要素と、OCO の遂行のための技

11 当該論点は、次を参照。Max Smeets, “Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment,” *Defence Studies*, vol. 18, no. 4 (August 2018), pp. 395–410.

12 次を参照。 Tobias Liebetrau, “Organizing Cyber Capability across Military and Intelligence Entities: Collaboration, Separation, or Centralization,” *Policy Design and Practice*, vol. 6, no. 2, (September 2022), pp. 131–145.

13 次を参照。Smeets, *No Shortcuts*, pp. 13–16; Daniel Moore, *Offensive Cyber Operations：Understanding Intangible Warfare* (Lomdom: Hurst Publishers, 2022), pp. 7–8, 69–100; Mikkel Storm Jensen, “Five Good Reasons for NATO’s Pragmatic Approach to Offensive Cyberspace Operations,” *Defence Studies*, vol. 22, no. 3, pp. 466–468.; Juliet Skingsley, *Offensive Cyber Operations: State’s Perceptions of their Utility and Risks*, Research Paper (London: Chatham House, September 2023), p. 6.

術の取得や利活用を支える専門人材、組織、制度等の非技術的要素の総体」を指す[14]。

以上の定義を整備 / 運用の概念に沿って整理すれば、MCF を含む国家機関が「整備」した OCC の「運用」により、サイバー空間を経由して任意の標的の情報資産に「4D」にあたる軍事的効果を創出する作戦行動が OCO となる。そのうえで、この OCO/OCC の概念については、次の 2 点の補足説明を必要とする。

第 1 に、ここでの OCO とは、軍事作戦の目的や国際法上の地位に従って整理された各国の政策文書やドクトリン上の共通見解を敷衍し、国毎の独自の用語法を捨象した学術研究上の概念である。重要な点は、講学上の概念である OCO に含まれる行為類型は、一般的に「サイバー攻撃」と呼ばれる行為より限定される。例えば標的のネットワークへの不正アクセスも、それが標的内部の機密情報の窃取に留まる限り OCO と扱われない。こうした情報資産の可用性や完全性を損なわず、あくまで機密性の侵害にのみ留まる行為は「コンピューターネットワーク搾取（CNE：computer network exploitation）」や「サイバー諜報活動（cyber espionage）」として C-ISR の一部と理解される。翻って「サイバー効果作戦（cyber effect operations）」とも通称される OCO は、伝統的に「コンピューターネットワーク攻撃（CNA：computer network attack）」と称される行為類型に相当する[15]。

第 2 に、概念上の区分にも係わらず、特定の OCO/OCC を支える技術・技巧は、攻撃側からは CNA/ サイバー効果作戦と CNE/ サイバー諜報活動の双方に活用しうる両用性を備えており、それゆえに防御側からは両者が外形的には識別困難なケースがある。それは、民間セキュリティ産業では「高度で持続的な脅威（APT：advanced persistent threats）」とも呼称される高度な標的型サイバー攻撃（以下：APT 攻撃）の場合である。APT 攻撃のキルチェーン（目標達成までのプロセス）は、標的への「4D」という効果創出を狙うか、標的からの情報窃取のみに留めるかに応じて最終段階で要求される技術・技巧の差異は生ずるが、それ以前のキルチェーンの構成技術・技巧は殆ど重複するからである[16]。

14 次を参照。*Ibid*, pp. 14, 73–92; Liebetrau, “Organizing Cyber,” p. 134; Florian J. Egloff and James Shires, “The Better Angels of Our Digital Nature? Offensive Cyber Capabilities and State Violence,” *European Journal of International Security*, vol. 8, no. 1, (February 2023), pp. 132–133; Winnona DeSombre, *A Primer on the Proliferation of Offensive Cyber Capabilities*, Issue Brief (Washington DC: Atlantic Council, March 2021), pp. 5–15.

15 以上の概念の区分のコンセンサスは、次を参照。Smeets, *No Shortcuts*, pp. 14–15; Jensen, “Five Good Reasons,” pp. 466–468; Skingsley, *Offensive Cyber*, p. 6.

16 APT 型攻撃のキルチェーンと、能力の諜報活動（CNE）と破壊工作（CNA）の間の両用性は次を参照。Timo Steffens, *Attribution of Advanced Persistent Threats - How to Identify the Actors Behind Cyber-Espionage* (Wiesbaden: Springer Vieweg, 2020), pp. 5–21, 24–26, 46; Smeets, *No Shortcuts*, pp. 14–15; Joe Devanny, Ciaran Martin, and Tim Stevens, “On the Strategic Consequences of Digital Espionage,” *Journal of Cyber Policy*, vol. 6, no. 3 (September 2, 2021), pp. 431–432.

（2）2つの OCC の類型に応じた異なる整備 / 運用と即応性確保の所要

イスラエル軍のサイバー作戦要員であったダニエル・ムーア（Daniel Moore）は、今日まで各国の軍事組織で整備 / 運用されてきた OCO/OCC を、「事前展開型（presence-based）」（以下：PBOCO/OCC）と、「局地事象型（event-based）」（以下：EBOCO/OCC）の 2 つの類型に区分する（表 1）。両者の最大の相違は、その能力の用途や潜在的な影響範囲と、即応性の確保に向けた能力整備上の所要に見出される [17]。

PBOCO/OCC は、先述の APT 攻撃の手法に相当し、その名の通り標的内部への侵入と潜伏による秘密裡のアクセスの獲得と維持を要する。ISR 活動に基づく攻撃手法の開発や踏み台とする中間標的からの水平移動等、最終標的へのアクセス獲得まで時に数か月から数年単位の準備を要すが、その反面、対象とする標的の地理的範囲や時期を調節し易く、かつ先述の APT 攻撃の両用性から、企業の知財窃取から重要インフラへの破壊工作まで、多様な政策目標の追求手段に供し得る柔軟性を備えた戦略級（strategic）の能力となる。

ただし個々の APT 攻撃の手法は、標的の環境に応じて必要な技術・技巧が異なり、継続的な新規取得や改良の要請が働くにもかかわらず、防御側の検知・対策や技術動向の変化を契機に短期間で無力化され易い特性を備える [18]。この特性を踏まえて PBOCC の即応性を維持するには、多様な攻撃手法の継続的な新規取得と改良、攻撃手法の運用保全（OPSEC：operational security）の徹底と無力化の防止、ある攻撃手法の無力化時の代替オプションの有無等も加味した投入対象や時期の調整といった「兵器庫管理（arsenal management）」とも通称される攻撃手法のライフサイクル管理への考慮が不可欠となる [19]。また、潜在的標的への事前の ISR 活動や、効果創出後の戦闘損耗評価（BDA：battle damage assessment）も含むターゲティング・サイクル（targeting cycle）[20] の各局面で、既存の INTEL が有する暗黙知を含めた技術・技巧に基づく組織的な支援が必要とされ易い。それゆえに PBOCC は、既存の INTEL から（軍

17 ムーアが類型化した PBOCO/OCC と EBOCO/OCC の定義と、その整備 / 運用の所要は次を参照。Moore, *Offensive Cyber*, pp. 7–8, 69–100.

18 こうした個々の攻撃手法の汎用性の低さと耐用期間の短さ（transitoriness）と呼ばれる特性については、次を参照。Max Smeets, “A Matter of Time: On the Transitory Nature of Cyberweapons,” *Journal of Strategic Studies*, vol. 41, no. 1–2 (February 23, 2018), pp. 6–32; Erica D. Borghard and Shawn W. Lonergan, “Cyber Operations as Imperfect Tools of Escalation,” *Strategic Studies Quarterly*, vol. 13, no. 3 (Fall 2019), pp. 122–145; Long, “A Cyber SOIP?” pp. 117-119; Smeets, No Shortcuts, pp. 116–122; Moore, *Offensive Cyber*, pp. 80–82.

19 Egloff and Shires, “The Better Angels,” p. 132; Max Smeets, “Cyber Arms Transfer: Meaning, Limits, and Implications,” *Security Studies*, vol. 31, no. 1 (February 2022), pp. 65–91.

20 軍事作戦の用語としての「ターゲティング（targeting）」の概念と、「ターゲティング・サイクル」の発想については、次を参照。Moore, *Offensive Cyber*, pp. 78–80; Paul Ducheine and Jelle van Haaster, “Fighting Power, Targeting and Cyber Operations,” in *6th International Conference on Cyber Conflict*, ed. P. Brangetto, M. Maybaum, and J. Stinissen (Tallinn: NATOCCDCOE, June 2014), pp. 320–323.

の）作戦部門に対する支援と、それを制度化するための両者間の組織的統合が、能力の即応性の獲得と維持の要件となる[21]。

他方で EBOCO/OCC は、前線の敵部隊が軍事作戦の遂行時に依拠する C4ISR 機能の妨害をはじめ、その用途と影響範囲が地理的または時間的に限定された目標達成を念頭に置く戦術級（tactical）または作戦級（operational）の能力となる。それゆえに EBOCO/OCC は、流動的な戦場の状況に直面する前線司令部や部隊単位での整備 / 運用の委任と自律性確保が、能力の即応性の確保に必要となる[22]。こうした分散自律型の運用構想を支える技術・技巧には、高度な例では、米陸軍の「サイバー・電磁波活動（CEMA：Cyber and Electro-Magnetic Activities）」の構想が念頭に置く、自動化された攻撃用のハード・ソフトウェアの電子戦兵器等への搭載と前線配備や、大隊以下の前線部隊での CEMA 専従部隊の編制等がある[23]。逆に高度な技術・技巧に依拠できない場合、DDoS 攻撃のように、技術的には陳腐でも、投入が比較的容易な攻撃手法の活用が志向される[24]。

またスミーツが実証してきたように、各国の政府機関による OCC の整備 / 運用の自由度は、各国の戦略目標や法令遵守の要請といった制約条件にも強く左右される[25]。例えば MCF が民主主義国の軍隊の一部である限り、シビリアンコントロールの原則に沿った軍事的合理性と政治目標との均衡の確保が求められる[26]。またマルチドメイン作戦（MDO：multi-domain operations）を含む、各軍種に跨る諸兵科との統合作戦や、同盟国との合同作戦（combined operations）の一部として OCO を遂行する場合、全体の目標や友軍の取組との役割分担も見据え、標的や効果創出の時期を調整する必要も生ずる[27]。更には民主主義国の法の下の行政の理念に沿って、軍事組織が各種の国際

21 本段落での PBOCO/OCC の整備 / 運用の所要の記述は、特に断りなき場合は次を参照。 Moore, *Offensive Cyber*, pp. 69–100.

22 特に前線の部隊支援のための OCO の展開における「ミッション・コマンド（mission command）」型の指揮統制メカニズムの要請は、次を参照。Franz-Stefan Gady and Alexander Stronell, “Cyber Capabilities and Multi-Domain Operations in Future High Intensity Warfare in 2030,” in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, ed. A. Ertan, et.al (Tallinn: NATOCCDCOE, December 2020), pp. 156–167; Issac R. Porche III et al, *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below* (Carifolnia: RAND Corporation, 2017), pp. 1-8, 47–75.

23 米陸軍を中心に発展してきた CEMA をめぐるドクトリンや関連構想の発展と、その具体化を支えてきた部隊・装備品は、次を参照。Stefan Soesanto, *A Digital Army: Synergies on the Battlefield and the Development of Cyber-Electromagnetic Activities (CEMA)*, CSS Cyber Defense Report (Zurich: Center for Security Studies of the ETH Zurich, August 2021), pp. 9–15, 20–31; Moore, *Offensive Cyber*, pp. 128–133.

24 本段落での EBOCO/OCC の整備 / 運用の所要の記述は、特に断りなき場合は次を参照。Moore, *Offensive Cyber*, pp. 69–100.

25 Smeets, *No Shortcuts*, pp. 36–37

26 当該論点は、次を参照。菊地茂雄「『軍事的オプション』をめぐる政軍関係―軍事力行使に係る意思決定における米国の文民指導者と軍人―」『防衛研究所紀要』第 16 巻第 2 号（2014 年 2 月）1–33 頁。

27 この点には、例えば 次を参照。Smeets, *No Shortcuts*, pp. 40–41; Long, “A Cyber SIOP?” pp. 105–128; Gady and Stronell, “Cyber Capabilities and Multi-Domain,” pp. 155–158.

表１　ムーアの類型化を踏まえた MCF による OCO/OCC の２つの類型

			事前展開型 OCO/OCC Presence-based [PB] OCO/OCC	局地事象型 OCO/OCC Event-based [EB] OCO/OCC
能力の用途と特徴			● 標的の範囲や効果創出の時期等の調節に長け、情報窃取から破壊工作まで多用途性を持つ戦略級の能力。	● 戦場を始め、地理的・時間的に限定された範囲で、標的の C4ISR 機能と意思決定の阻害に特化した戦術級の能力。
即応性の確保・維持の所要			● 組織間統合等を通じた、能力整備 / 運用の基盤を握る既存の INTEL から軍の作戦部門に対する支援の制度化。	● 攻撃手法の事前配備や権限の下位の司令部・部隊への委任等を通じた、前線における能力整備 / 運用の自律性の確保。
類似の機能を備えた作戦でのアナロジー			インテリジェンス機関による非公然工作（covert action）	軍による戦場での火力支援（Fire supports）
効果創出までのプロセス	1	準備（Preparation）	● 多様な戦略目標や標的を念頭に置いた、広範囲に渡るターゲティングと能力開発。	● 局地的戦場での戦術単位での標的への効果創出に向けたターゲティングと能力開発。
	2	接敵（邂逅）（Engagement）	● 効果創出前に標的への侵入と秘密裡のアクセス獲得を要請。侵入手法は多様だが、標的間の水平移動や潜伏の要請から長期化傾向。	● 前線部隊における運用が念頭にあり、接敵手法は攻撃のツールと標的の特定機器の間のみで短期間で完結する傾向。
	3	事前展開（Presence）	● 標的間の水平移動と潜伏による秘密裡のアクセス維持が要請され、作戦の地理的範囲と期間が拡大傾向。 ● 事前に獲得した秘密裡のアクセスは標的の情報窃取と破壊工作の双方に活用可。	● 標的間の水平移動や標的内における長期間の潜伏維持の要請は限定的または不要。攻撃ツールの標的に対する投射（接敵）の後、効果創出まで短期または即座に完結。
	4	効果創出（Effects）	● 地理的・時間的・機能的な広がりを持つ戦略的含意。	● 地理的・時間的範囲や機能が限定された戦術的含意。
具体的な攻撃手法（技術・技巧）			● 高度標的型サイバー攻撃（いわゆる APT 型攻撃）	● 電子戦兵器に搭載可能な自動化された攻撃ツール ● DDoS 攻撃 ● 簡素な Wiper 型マルウェア

（出所）以下の各文献を参照し執筆者作成。Moore, *Offensive Cyber*, pp. 69–100, 117–144, 245–249; Smeets, *No Shortcuts*, pp.13–16, 73–92; Gady and Stronell, “Cyber Capabilities and Multi-Domain,” pp. 156–167. ; Soesanto, *A Digital Army*, pp. 5–32. ; Porche Ⅲ et.al, *Tactical Cyber*, pp. 1–8, 47–75.

法・国内法令等の遵守の要請に服する限り、能力整備のために軍事組織が取りうる措置の範囲や、比例性 / 均衡性等を考慮した OCO の標的選定の対象、効果創出の範囲や付随的損害の局限の要否も左右する [28]。

特に民主主義国家の場合、上述のような「兵器庫管理」の要請や、更には戦略目標や法令遵守の要請といった制度上の制約を加味し、その投入時期や影響範囲を統制しうる OCC の即応性を獲得し、維持し続ける必要がある。こうした能力整備 / 運用の要求水準は、国家が自身の OCC の整備 / 運用の過程を信頼し得ないサイバー犯罪集団等に外部委託する余地を狭め、むしろ能力整備 / 運用の内製化に向かわせる誘因を生じさせることになる [29]。

（3）OCC の整備 / 運用における既存の INTEL の機能と MCF の固有性の問題

MCF による OCC の整備 / 運用は、現実には MCF とそれ以外の主体との関係も含めた各国の政策過程内でのガバナンスの問題でもある。ここで特に問題となるのは、軍事組織の一部として OCO という作戦の遂行を司る MCF と、既存の INTEL という、異なる中核任務と組織文化を体現する政府組織間の関係性にある。歴史的には表 1 の PBOCC に該当する能力の整備 / 運用は、今日 MCF と称される軍事組織の台頭以前に、Civ-INTEL を含む SIGINT を担う INTEL が必要な基盤を提供してきた [30]。またノルウェーのように、既存の軍系統のインテリジェンス機関（Mil-INTEL：military intelligence）が OCO の遂行権能を一元化され、本稿の定義上の MCF の地位を備える国もある [31]。こうした事例を踏まえて生ずる問いは「なぜ一部の国は、既存の INTEL の権限や資源の単純な拡大ではなく、あえて別個に MCF を編制して OCC の整備 / 運用を担わせる制度選択をするか」である。そもそも国家が OCC の整備 / 運用を追求するにせよ、既存の INTEL の存在にもかかわらず、あえて MCF を別個に新編して担わせる必要があるのかは必ずしも自明ではない。これが、本稿が「二重の統合仮説」を通じた事例研究を通じて明らかにしたい問いとなる。

（4）本稿における「二重の統合仮説」の含意

ここで改めて、本稿における「二重の統合仮説」の含意を明確化する。序論で触れ

28 次を参照。Smeets, *No Shortcuts*, pp. 36–42; Gady and Stronell, “Cyber Capabilities and Multi-Domain,” pp. 164–165, 167.
29 国家による非国家主体に対する OCC の整備 / 運用の外部委託のリスクと限界をめぐる議論は、次を参 照。Smeets, *No Shortcuts*, pp. 8–10, 147–161.
30 例えば、米英については次を参照。Robert M. Chesney, “Adapting to the Cyber Domain: Comparing US and UK Institutional, Legal, and Policy Innovations,” *Aegis Paper Series*, no. 2013 (May 2021), pp. 5–6, 19–25.
31 Liebetrau, “Organizing Cyber,” pp. 138–140.

たように、本稿での「(二重の) 統合」とは、「軍種間の統合 (joint)」よりも広義の一般的用法を念頭に、具体的に「第 1 の統合」と「第 2 の統合」の 2 軸からなる。

「第 1 の統合」は、現代の複雑な軍事作戦に対する OCC の「統合 (integration)」を含意する。これは具体的には MCF が、OCC を、文民の政治指導者、複数軍種に跨る諸兵科の部隊、インテリジェンス・コミュニティ (IC：intelligence community) を含む関係省庁、そして同盟国の機関といった多様な利害関係者が関与する軍事作戦の全体のピースの一部として機能しうる状態に置くことを指す。これは例えば OCC の整備 / 運用に必要な専門人材の採用と訓練・演習を通じた維持や各種の資機材の調達に留まらず、MCF と各軍種・関係省庁・同盟国等との間での共同作戦計画や指揮統制メカニズムの構築といった膨大な政策調整を伴う[32]。この点は軍事組織の指揮系統外の Civ-INTEL は勿論、軍事組織の一部である Mil-INTEL も、INTEL としての政策形成や執行からの中立性の規範ゆえに大規模な政策調整の当事者としては適格ではないとの仮定を置くと、MCF という別個の軍事組織を受皿として、政策調整の工程管理に責任を負わせる要請が生ずるとの仮説が成り立つ。

次に「第 2 の統合」は、特に 2000 年代の対テロ戦争期の先行研究で「作戦・インテリジェンス統合 (operation-intelligence fusion)[33]」と表現されてきた概念に相当する。これは例えば共同の部隊や合同調整所等を通じた INTEL 要員と作戦部門の要員の実働での協力により、既存の INTEL の能力のターゲティング・サイクルにおける活用といった「運用 (作戦) に対する情報支援 (intelligence support for operations) (以下：運用情報支援)」を強化することを指す[34]。ジョン・リンゼイ (John Lindsay) をはじめ、OCO と、伝統的な特殊作戦 (special operations) や非公然工作との機能面の連続性を捉える先行研究[35]からは、表 1 の PBOCC の整備 / 運用でも同様の所要が生ずるとの仮説が成り立つ。

また本稿の「第 2 の統合」とは、個々の OCO を支える運用情報支援を超えた、連携の累積を通じた軍の作戦部門と INTEL の間での能力整備 / 運用をめぐる方針や組織文化の溝の克服も含意する。INTEL は、特に Civ-INTEL を中心に、軍の作戦部門

32 OCO をめぐる共同作戦計画や指揮統制の論点は特に次を参照。Long, “A Cyber SOIP?” pp. 105–128; Smeets, *No Shortcuts*, pp. 40–41, 87–92; Gady and Stronell, “Cyber Capabilities and Multi-Domain,” pp. 156–158; Jensen, “Five Good Reasons,” pp. 470–482; Porche III et al., *Tactical Cyber*, pp. 1–8, 47–75.

33 John Hardy, “Hunters and Gatherers: The Evolution of Strike and Intelligence Functions in Special Operations Forces,” *International Journal of Intelligence and Counterintelligence*, vol. 36, no. 4 (October 2023), p. 1146.

34 次を参照。Ibid., pp. 1146–1163; Porche III et al., *Tactical Cyber*, pp. 9–22.

35 次を参照。Jon R. Lindsay, “Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem,” *Intelligence & National Security*, vol. 36, no. 2 (February 2021), pp. 260–278; Rory Cormac, *How To Stage A Coup – And Ten Other Lessons from the World of Secret Statecraft* (London: Atlantic Books, 2022), pp. 232–251.

との相対比較では標的への効果創出（OCO/CNA）には消極的な組織文化を形成し易い[36]。なぜなら「4D」という効果創出は、防御側の検知と対応を惹起し易く、それは同一の標的に秘密裡に行われるサイバー諜報活動 /CNE も含め、「（軍を超えた）政策決定者の意思決定支援」という中核任務にも供し得る機微な情報収集源の喪失に繋がるリスクが高いからである[37]。

これを軍の作戦部門の立場から捉えると、既存の INTEL が抱える効果創出への消極性を緩和しつつ、INTEL から自身の OCO/CNA に必要な「運用情報支援」を引き出すメカニズムの制度化が必要となる。言い換えれば、既存の Civ-INTEL/Mil-INTEL の要員を転用しつつも、あえて INTEL の本体とは別個に編制された MCF とは、能力整備 / 運用をめぐる平素からの実務協力の過程で、両者間に生じる能力整備 / 運用方針や組織文化の相違を克服するための装置であるとの仮説が成り立つ。

以上が「二重の統合仮説」の含意となるが、現実に各国の政策過程で、そうした機序が INTEL とは別個の MCF の新編要因として存在してきたかは、必ずしも実証されてはいない。こうした課題を背景に、第 2 節以降では米国とオランダの 2 か国の MCF に焦点を絞った比較事例研究を通じて、「二重の統合仮説」の想定する因果メカニズムが、両国の 2010 年代以降の両国の MCF の動向に見出しうるか否かに着目した過程追跡を試みる。

3．事例研究のリサーチデザイン

本稿の事例研究が扱う問いを再確認すれば、「なぜ特定の民主主義国の政府における OCC の整備 / 運用は、（理論上は可能な）既存の INTEL の資源 / 権限の拡大と集権化ではなく、MCF という別個の軍事組織の関与を通じて追求されるのか」と表現できる。これを踏まえて本稿では、民主主義国の MCF は、OCC の軍事力としての即応性の確保の観点から（1）「第 1 の統合」（軍事作戦の一部としての OCC の組込）と、（2）「第 2 の統合」（INTEL による軍の作戦部門への支援の合理化と両者間の組織文化のギャップの克服）の 2 つの意味の「統合」が必要となり、同時に、この 2 つの「統合」を促

36 当該論点は次を参照。Lindsay, “Cyber Conflict,” pp. 268–271; Joe Devanny et al., *The National Cyber Force that Britain Needs?* Report (London: Kings Colledge London, April 2021), pp. 10–11; Moore, *Offensive Cyber*, p. 71; Max Smeets, “Integrating Offensive Cyber,”, pp. 395–410.

37 当該論点は次を参照。Max Smeets, “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection,” *Intelligence & National Security*, vol. 35, no. 3 (April 2020), pp. 444–453; Danny Steed, *The National Cyber Force: Directions and Implications for the UK*, ARI 18/2021 - 9/2/2021 (Madrid: The Elcano Royal Institute) pp.4–5.

す装置として既存の INTEL とは別個の MCF が編制されると捉える「二重の統合仮説」を設定する。

本稿の事例研究では、2010 年代以降、米軍[38]とオランダ軍[39]の隷下で OCC の整備 / 運用を任務とした MCF の動向を観察し、「二重の統合仮説」の想定する因果メカニズムがどの程度まで妥当するかを明らかにする。本稿では定性的事例研究での決定的事例研究の方法論[40]を意識し、米蘭の 2 か国の MCF のうち、特に以下のケースに焦点を絞って分析する。

米国の事例は、過激派組織「イラク・レバントのイスラム国（ISIL）」に対し、米国中心の有志連合軍が 2014 年から展開してきた軍事作戦である「生来の決意作戦（OIR：Operation Inherent Resolve）[41]」の支援目的で展開された一連の OCO を扱う。本稿では、特に 2016 年 5 月頃に米国サイバー軍（USCYBERCOM）の司令官が編制した統合任務部隊 ARES（以下：JTF-ARES）が、数か月間の調整期間を経て、同年 11 月に開始した「輝かしき交響曲作戦（OGS：Operation Glowing Symphony）」と呼ばれる全世界規模での一連の OCO を分析対象とする。

この事例では、ISIL に対する統合 / 連合作戦における OCC の整備 / 運用の要請を背景に生起した JTF-ARES の「新編」の経緯と、JTF-ARES での能力整備 / 運用の過程を詳細に観察できる。米軍による ISIL への軍事作戦は、2014 年以降、米国主導の有志連合軍による OIR の枠組で進展し、USCYBERCOM は 2016 年まで、この OIR の指揮統制メカニズムの下で OCO の遂行により OIR を支援してきた。既存の実績にも係わらず、USCYBERCOM が JTF-ARES の新編と OGS の展開に至った事実は、OCC の整備 / 運用上の要請が MCF の新編 / 改編を導くとの本稿の仮説の想定が該当する典型的事例の過程追跡を可能とする。

第 2 の事例研究は、2010 年代から 2023 年 12 月時点までのオランダ軍隷下の MCF の新編 / 改編と、OCC の整備 / 運用への取組の観察となる。本稿では特に 2010 年代中盤に新編された国防サイバーコマンド（DCC：Defensie Cyber Commando）と、2021 年、DCC とは別個に陸軍隷下に新編されたサイバー・電磁波活動中隊（Cyber & Electric Magnetic Activities Compagnie）（以下：NLA-CEMAC）を分析対象とする。

38 本稿の米軍の各組織や指揮統制上の用語の訳語は、別途定訳として確立した表現がある場合を除けば、次の文献を参照。山下隆康「米軍の指揮統制関係」『防衛研究所紀要』第 21 号第 1 巻（2018 年 12 月）211–245 頁。

39 本稿で引用する蘭政府・議会等の文書につき、英語版が利用可能な場合、蘭語原文の公表時期を示しつつも内容に相違が無い場合は英語版から引用する。蘭語版のみ存在する史資料は、翻訳確認時に 2 次資料を参照した場合は併記する。また固有名詞は、通例蘭語表記されるものは本文中も蘭語表記を用いる。

40 野村康『社会科学の考え方－認識論、リサーチデザイン、手法』（名古屋大学出版会、2020 年）47–76 頁。

41 OIR の全体像は次を参照。Andrew Mumford, *The West's War against Islamic State* (London: I B Tauris, 2022), pp. 9–80.

両事例は、蘭軍内で異なる条件を備えた MCF の時系列的な事例内比較を可能とする。DCC は上述の JTF-ARES の事例と異なり、創設時点で切迫した軍事作戦の要請に直面してきた事実は必ずしも確認できない。この条件下でも DCC が「第 1 の統合」と「第 2 の統合」の機序に従って発展してきた事実を観察できれば、仮説への支持は一層強くなる。また NLA-CEMAC は、DCC とは別個に 2021 年に新編され、限られた公開情報に照らす限り、ムーアが指摘する EBOCC の整備 / 運用を目指す形跡が見て取れる。こうした事例の「2 重の統合仮説」に対する示唆を捉えることが、同事例を観察対象に加える意義となる。

また上記の米蘭 2 か国の事例間比較は、次のような実証面での優位性を持つ。第 1 に、米蘭両国は共に NATO 加盟国かつ民主主義国として、OCC を含む軍事力の整備 / 運用をめぐる法令遵守やシビリアンコントロールの要請に服する [42]。この点、両国は第 2 節で触れた OCC の整備 / 運用の制約条件となる政治体制の影響を統制した上での比較を可能とする。第 2 にオランダは、特に米英両国とのインテリジェンス協力が緊密な NATO 加盟国であり、C-ISR や OCO のための能力整備 / 運用でも、既に 2010 年代中頃からの運用面の協力や、後に見る通り特に蘭側による米側の先進事例の吸収の試みも確認できる。この条件は、例えば米蘭両国の国際情勢や脅威認識といった変数の統制に資すると共に、限定的ではあれ、米蘭の 2 か国間協力の内容を通じた蘭側の MCF の取組の意図も推論も可能とする。

最後に、仮説の当否を問わずして、上記の米蘭両国の MCF に着目した定性的な事例研究を行う意義を述べたい。本稿が挙げる米蘭の両事例は、両国政府により機密指定解除がなされた行政文書や議会証言等の活用を通じ、米蘭両国という民主主義国の MCF が、両国の国内政治過程や同盟国等との対外関係の相互作用の下で OCC の整備 / 運用を進める際に直面する課題を観察できる。こうした稀有な事例にも係わらず、管見の限り同様の史資料を用いた学術研究は国内では絶無である。この点で本稿は、従来の国内の学術研究や政策論争が捉えてこなかった、オランダのような「中小国」を含めた「自由民主主義国」の MCF が OCC の整備 / 運用に際して直面する固有の課題を炙り出す。この作業は従来の「国家のサイバー攻撃」の議論が、専ら米中露のような超大国や、北朝鮮のような権威主義国家のケースを念頭に置いてきたことのサンプリング・バイアスを是正する意義を持つ。

42 米蘭両国の OCC の整備 / 運用をめぐる根拠法令や統制のメカニズムの概要は、次を参照。Skingsley, *Offensive Cyber*, pp. 24–25.

4．USCYBERCOM による過激派組織 ISIL への OCO の事例研究

（1）USCYBERCOM による ISIL への OCO の推移：「支援」から「主導」への転換

米軍が過激派組織 ISIL に展開してきた一連の OCO は、USCYBERCOM や各軍種のサイバーコマンドの任務の性質や指揮統制メカニズムに着目すると、大きく次の 2 段階に整理できる。

第 1 の段階は、「支援期間」と呼称しうる、2014 年 10 月頃の OIR 始動後から JTF-ARES が新編される 2016 年 5 月頃までの期間となる。米国国家安全保障アーカイブ（NSARC：The National Security Archive）所収[43]の 2015 年 3 月 29 日付の「作戦命令 15-0055（OPORD[Operations Order] 15-0055）[44]」や翌 2016 年 4 月 12 日付の「任務分析報告（MAB：Mission Analysis Brief）[45]」といった行政文書群[46]を踏まえる限り、この「支援期間」では、合同統合任務部隊 OIR（CJTF-OIR：Combined Joint Taskforce OIR）の基幹を為す米国中央軍（USCENTCOM）に対し、主に米陸軍サイバーコマンド（ARCYBER）が OCO を含む各種 CO によるイラク・シリアでの軍事作戦への支援を提供しつつ、USCYBERCOM 本体も、USCENTCOM の担任地域外での OCO を含め、一定の作戦行動に関与してきた形跡が見られる[47]。

第 2 の段階は、2016 年 5 月の JTF-ARES の編制を始点に、この JTF-ARES を軸に 2016 年 11 月以降に OGS が実際に展開された期間を指す。本稿ではこの段階を、第 1 段階との対比で「主導期間」と呼称する。「支援期間」から「主導期間」への移行に伴い、既存の CJTF-OIR とは別個に、USCYBERCOM 司令官の権限に基づき、統合任務部隊 JTF-ARES が新編された。この JTF-ARES を軸とした指揮統制メカニズムの下で、ISIL のメディア運営や外国人戦闘員獲得の基盤として全世界に散在する ICT インフラの壊滅を主目的とする一連の OCO としての OGS が展開されていった。

---

43 2023 年 12 月現在までに機密指定解除済の行政文書群は、Ns-ARCH の公式のページから確認できる。Michael Martelle, “Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command’s Internet War Against ISIL,” National Security Archive, August 13, 2018, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil; Michael Martelle, “USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY,” National Security Archive, January 21, 2020, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.

44 USCYBERCOM, “USCYBERCOM Operations Order（OPORD）15-0055: Operations Order in Support of Operation Inherent Resolve, March 29, 2015,” Cyber Vault Library of the National Security Archive.

45 USCYBERCOM, “United States Cyber Command, Mission Analysis Brief: Cyber Support to Counter ISIL, April 12, 2016. Unclassified,” Cyber Vault Library of the National Security Archive.

46 以下で引用する NSARC 所収の行政文書の引用ページは、原典文書毎に記載のフォーマットが異なるため、原則として NSARC で電子化された PDF データのページ番号に従い記載する。

47 USCYBERCOM “OPORD 15-0055,” pp. 2–4, 8–10; USCYBERCOM, “Mission Analysis Brief,” pp. 2–6, 14–15, 36–38.

先の MAB を含む各種史資料では、この JTF-ARES の新編は、USCENTOCM を軸とする CJTF-OIR の担任地域を超える地理的範囲における OCO の拡大や、IC を含む関係省庁や同盟国との調整機能の強化を通じた、ISIL に対する OCO で創出しうる軍事的効果の増幅の要請から導かれている[48]。こうした JTF-ARES の新編を裏付けた軍事的合理性の存在を前提に、JTF-ARES が、OGS の開始前後の期間で ISIL を念頭に置く能力の整備 / 運用のための「二重の統合」の機能を果たしてきたかを確認する。

（2）JTF-ARES による「第 1 の統合」の促進

2016 年 5 月 5 日付の JTF-ARES の編制命令文書[49] に基づき、JTF-ARES には ISIL の活動を支える ICT インフラへの攻撃ツールの取得と運用のほか、OGS の遂行に必要な作戦計画の策定や運用時の衝突回避（deconfliction）をめぐる関係諸機関との調整任務が付与された[50]。ここでの JTF-ARES の調整対象は、主に次の 3 つのカテゴリに整理できる。

第 1 には、OIR の指揮統制メカニズムの下での軍事作戦に関与してきた米軍の地域別および機能別戦闘軍である。特にイラク・シリア両国の地上部隊支援のための空爆を担う USCENTCOM や、同地での特殊作戦等に関与する米国特殊作戦軍（USSOCOM）との間では、ターゲティングの調整要領が存在し、JTF-ARES と USCENTCOM や USSOCOM との間の連絡官の相互派遣や連絡会合の存在も記載がある[51]。これらの取組を通じて JTF-ARES は、イラク・シリアの領域内での軍事作戦の展開も見据え、OCO の標的選定や効果創出の時期をめぐる調整と同期を図ってきた。

第 2 には、米国大統領府や国務省を含めた米国政府内の関係省庁である。2016 年 12 月 13 日付の OGS 開始後 30 日段階のレビュー文書に照らす限り、JTF-ARES は OGS の初期の作戦計画の策定後に、「統合的関係省庁間調整（JIC：Joint Interagency Coordination）」と呼ばれるメカニズムを通じて国内関係省庁との調整に従事してきた[52]。この JIC での調整は、上記のレビュー文書と各種の調査報道の内容を照らし合わせる限り、ISIL が利活用する ICT インフラで何を打撃対象とすべきかという標的選定の選択肢の議論に始まり、例えば ISIL の利用するサーバーが同盟国の管轄権内で設

48 USCYBERCOM, “Mission Analysis Brief,” pp. 6, 23–38; Martelle, “Joint Task Force ARES.”
49 USCYBERCOM, “USCYBERCOM to CDRUSACYBER, Subj: CYBERCOM FRAGORD 01 to TASKORD 16-0063 To Establish Joint Task Force (JTF)-ARES to Counter the Islamic State of Iraq and the Levant（ISIL）in Cyber Space, May 5, 2016. Secret//Rel to USA, [Redacted],” Cyber Vault Library of the National Security Archive.
50 Martelle, “Joint Task Force ARES.”
51 Ibid.; USCYBERCOM “FRAGORD 01 to TASKORD 16-0063,” p. 36.
52 USCYBERCOM, “USCYBERCOM 30-Day Assessment of Operation Glowing Symphony, December 13 2016. Top Secret,” Cyber Vault Library of the National Security Archive, pp. 9–10, 15–17.

置されている場合、OCO の遂行前に当該国への事前通報と同意を要するかといった、JTF-ARES による OCO の遂行における具体的な交戦規定の問題にまで及んでいる[53]。

最後に、OGS に参加する有志連合国の機関である。USCYBERCOM の文書内での JTF-AREs の指揮系統図[54]や、当時の USCYBERCOM 司令官のマイケル・ロジャース（Michael Rogers）の証言を踏まえると、JTF-ARES は、英国と豪州といったファイブアイズ諸国を筆頭に、有志連合国との緊密な調整下で OGS を遂行してきた[55]。例えば 2016 年 10 月 7 日付の USCYBERCOM の行政文書を見ると、JTF-ARES は有志連合国との間で、OCO による打撃対象の分担や運用時の衝突回避の調整も図っている[56]。また 2016 年 11 月 4 日付の文書からは、オランダの機関が、JTF-ARES の一定の作戦行動に伴う事前通報の窓口に指定されてきた点も読み取ることができる[57]。

（3）JTF-ARES による「第 2 の統合」の促進

OGS 開始後 120 日段階のレビュー文書の記述からは、JTF-ARES の調整対象は、USCYBERCOM 司令官隷下の国家安全保障局（NSA）に留まらず、米国中央情報局（CIA）や、米国連邦捜査局（FBI）を所管する米国司法省（DoJ）も含めて、米国の IC の主要構成官庁にまで及んだことがわかる[58]。こうした JTF-ARES と IC との調整は、具体的には OGS の遂行過程の以下の局面で重要となった。

第 1 には、OCO のターゲティング・サイクルを支える各種の運用情報支援である。例えば、JTF-ARES は 2016 年 5 月の発足段階から、ISIL 要員が利用するウェブサービスのアカウントやサーバー等の情報資産を標的とする ISR 活動と攻撃手法の開発に従事してきた[59]。この段階で JTF-ARES は、USCYBERCOM の情報部（J2）要員を充

53 NSARC 所収の史資料と以下のエレン・ナカシマ（Ellen Nakashima）の調査報道を照らし合わせる限り、関係各省間の数週間の協議の紛糾を経て、最終的には標的所在国である約 35 か国のうち、同盟国を含む約 15 か国に所在する標的への OCO をめぐる事前通知方針が採用された。Ibid.; Martelle, “USCYBERCOM After Action Assessments”; Ellen Nakashima, “U.S. Military Cyber Debate over Alerting Allies,” *The Washington Post*, May 8, 2017.

54 USCYBERCOM, “USCYBERCOM 30-Day Assessment,” p. 4.

55 ロジャースによる JTF-ARES を通じた米英豪との連携への言及は、以下音声記録の 27:00-29:00 を参照。Shawna Sinnott and Abigail Gage, “Cyberspace as a Battlespace: Irregular Warfare Through Bits and Bytes,” *Irregular Warfare Podcast*, November 19, 2021.

56 USCYBERCOM, “In Progress Review OP Glowing Symphony [Redacted], October 7 2016, Secret,” Cyber Vault Library of the National Security Archive, pp. 17–18; Martelle, “Joint Task Force ARES.”

57 Department of Defense, “Agreed Operation Glowing Symphony Notification Plan, November 4 2016, Top Secret,” Cyber Vault Library of the National Security Archive, pp. 1–2.

58 USCYBERCOM, “USCYBERCOM 120-Day Assessment of Operation Glowing Symphony, April 12 2017. Top Secret,” Cyber Vault Library of the National Security Archive, pp. 10, 15–16.

59 ISIL の運用するサーバーや SNS アカウント等への ISR 活動も含めた一連の能力整備 / 運用の過程は、以下を参照。Martelle, “Joint Task Force ARES”; Dina Temple-Raston, “How The U.S. Hacked ISIS,” *NPR*, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

てた「インテリジェンス統合セル（intelligence fusion cell）[60]」を窓口として IC と相互に情報要求を伝達し、米国の IC の関係機関から OGS の準備段階での ISR 活動への協力を取り付けている [61]。また、標的への OCO/CNA の実施後の BDA についても、米国や有志連合への参加国の作戦行動が所期の効果を達成したか否かの評価を IC が実施した形跡が存在する [62]。

第 2 には、標的に対する効果創出に伴うインテリジェンス得失（IGL：intelligence gain/loss）の評価共有を含めた衝突回避の局面である。各種の史資料からは、この局面が JTF-ARES と IC の構成官庁間の調整の最大の争点となった点が見てとれる。例えば前項で触れた JIC では、JTF-ARES が当初提示した標的への OCO の実施計画について度々 INTEL 側から情報源の損失のリスクに伴う懸念の表明と異議申立てが行われてきた [63]。OGS 開始後 30 日のレビュー文書と調査報道の内容からも、JTF-ARES が、JIC での INTEL の消極的姿勢を緩和し、作戦計画への合意を調達するため、実務者級から国家安全保障会議での各省高官級の協議までを含めた、様々な連絡会合への対応に多大な調整コストを払ってきたことが見て取れる [64]。

以上のように JTF-ARES は、IC を含む多様な関係省庁を OGS の作戦計画の策定段階から関与させつつ、自身の OCC の整備 / 運用の過程の一部に組み込もうとしてきた。これによる作戦の始動時期や個別の標的選定への容喙を甘受してなお、JTF-ARES が JIC を通じた関係省庁間調整に関与せざるを得なかった事実は、同盟国の管轄地域も含め、全世界規模で展開する OGS での OCC の整備 / 運用に際して、軍事的合理性と政治的目標との均衡の確保と、IC からの運用情報支援の獲得の必要性が関係当事者の間で内面化されてきたことを示す。この事実は、本稿の「二重の統合仮説」を強く支持するものとなる。

60 USCYBERCOM, “FRAGORD 01 to TASKORD 16-0063,” p. 36.
61 Ibid.; USCYBERCOM, “USCYBERCOM 30-Day Assessment,” pp. 19–21.
62 USCYBERCOM, “USCYBERCOM 30-Day Assessment,” pp. 2, 8–9.
63 こうした IC 側の抵抗については、次を参照。USCYBERCOM, “USCYBERCOM 120-Day Assessment,” pp. 15–16, 20; Ashton Carter, *A Lasting Defeat: The Campaign to Destroy ISIS*, Special Report (Cambridge: Belfer Center for Science and International Affairs of the Harvard Kennedy School, 2017), pp. 32–33.
64 USCYBERCOM, “USCYBERCOM 30-Day Assessment,” pp. 15–17.；Nakashima, “U.S. Military Cyber,”.

5．オランダ軍による OCC の整備 / 運用の事例研究

（1）2010 年代前半のオランダ国防サイバーコマンド（DCC）の発展と蹉跌

DCC は、蘭国防省が 2012 年 6 月刊行の「国防サイバー戦略」（以下：DCS2012[65]）に基づき新編が決定され、蘭国防省内における準備作業を経て 2015 年 6 月に陸軍の一部として実働開始、2018 年 7 月以降は蘭軍参謀総長の直轄コマンドに格上げされて現在に至る [66]。この DCC による OCC の整備 / 運用の指針は、組織の新編を定めた DCS2012 にその起源を見ることができる。

DCS2012 は、その本文で「攻勢的サイバー能力（offensive cyber capability[67]）」を蘭軍による軍事作戦の戦力増幅機能を担う能力と位置付け、当該能力の「展開の即応性の維持」を担う組織としての DCC の新編を決定しており、かつ蘭軍の軍事作戦の遂行時、憲法と法令で定められた参謀総長の指揮命令権限に沿って、DCC が保持する OCC を行使するとの記述を含む [68]。このように DCC が、蘭軍の軍事作戦の支援の観点から OCC の整備 / 運用を担うことは、その後も DCS2012 をめぐる蘭国防大臣の議会での言及のなかで、繰り返し DCC による OCC の整備 / 運用の一貫した方針として示されてきた [69]。

その後も DCS2012 の内容をめぐる蘭国防省や DCC の説明は、DCC が OCC の整備 / 運用に際して、PBOCC に相当する能力の所要を念頭に置きつつ、軍情報保安局（MIVD）の資源を活用することや [70]、DCC が蘭軍展開時の作戦司令部に対する OCC の統合を促すアドバイザー機能を果たすことにも触れている [71]。一連の言及は、DCC が新編当初より、「二重の統合」の促進を企図してきたことを示唆するものといえる。

65 Netherlands Ministry of Defence (hereafter NLMOD), *The Defence Cyber Strategy*, June 27, 2012; Matthijs R. Koot, “The Dutch Defense Cyber Strategy of 2012,” *Matthijs R. Koot’s Notebook (Blog)*, July 18, 2012, https://blog.cyberwar.nl/2012/07/nl-uk-translation-of-the-dutch-defense-cyber-strategy/.

66 2012 年 6 月以来の DCC 創設に向けた組織的沿革は次を参照。Smeets, *No Shortcuts*, p. 67.

67 NLMOD, *The Defence Cyber Strategy*, pp. 6, 8, 11. なお蘭語では “offensieve cybercapaciteiten” と表現され、この表現は蘭語版の『DCS2012』やその後の蘭議会での政府側の説明等でも用いられている。

68 *Ibid*., p. 11.

69 例えば 2014 年 3 月 17 日付で、当時の国防相がオランダ第 2 院（Tweede Kamer der Staten-Generaal）に宛てた書簡は、『DCS2012』の記述に基づく DCC による OCC の整備 / 運用の基本方針と進捗状況を説明している。*Brief Van De Minister Van Defensie*, Kamerstuk 33321 nr. 3: Defensie Cyber Strategie, Vergaderjaar 2013–2014, pp 1–4, https://zoek.officielebekendmakingen.nl/kst-33321-3.pdf; Matthijs R. Koot, “Progress of Offensive Cyber Capabilities in the Netherlands’ Armed Forces,” *Matthijs R. Koot’s Notebook (Blog)*, March 18, 2014, https://blog.cyberwar.nl/2014/03/progress-of-offensive-cyber-capabilities-in-the-netherlands-armed-forces/.

70 Matthijs R. Koot, “Speech by Dutch Secretary of Defense at Cyber Symposium on June 27th 2012,” *Matthijs R. Koot’s Notebook (Blog)*, July 17, 2012, https://blog.cyberwar.nl/2012/07/speech-by-dutch-secretary-of-defense-at-cyber-symposium-on-june-27th-2012/; Kamerstuk 33321 nr. 3, pp. 2–3.

71 Hans Folmer, “Defensie Cyber Commando, Een nieuwe loot aan de Defensieboom,” *Operationeel: Intercom*, vol. 45, no. 1 (2016), pp. 25–28.

ただし DCS2012 の指針に沿った OCC の整備 / 運用が、DCC の新編後に必ずしも順調に進んできた訳ではない。例えば第 2 代 DCC 司令官エレノア・バークホルト・オサリヴァン（Elanor Boekholt-O'Sullivan）は、DCC は 2018 年末の段階でもなお各種権限不足の問題に直面し、単独では OCC の整備 / 運用が不可能な状況にあったと認めた[72]。各種のインタビュー調査を踏まえ、この状況を裏付けたスミーツやアレクサンダー・クラバー（Alexander Claver）の先行研究は、その主な要因として、DCC が OCC の整備 / 運用に不可欠な平素からの ISR 活動の法令上の権限を有しえなかった点や、この運用権限の欠缺に伴う実践（戦）を通じたスキルアップの機会の乏しさが、DCC の内部での OCC の整備 / 運用に不可欠な専門人材の採用・育成・維持の取組を困難にしたことを挙げている[73]。

以上の DCC が単独での能力整備 / 運用基盤を欠く状況は、2018 年当時から既に当局者間では公知の事実であった[74]。しかし、2010 年代後半の国防相の関連答弁やセルゲイ・バーク（Sergei Boeke）の先行研究を踏まえても、この DCC の法的権限の欠缺の問題に、立法政策上の是正を試みた形跡は見てとれない[75]。またスミーツによる蘭国防省関係者へのインタビュー調査は、2010 年代前半の時点では、DCC は当時の国防予算削減圧力と親和的な形で効率的な軍近代化が可能な新領域の戦力と期待されており、それゆえに当局者の見積上も能力整備 / 運用の所要が必ずしも厳密に把握されてきた訳ではない点も示唆する[76]。一連の事実を捉える限り、2010 年代前半の DCC は、必ずしも「二重の統合仮説」の機序に従って発展した訳ではなく、国内政治的な論理と既存の法制度の経路依存性のなかで規定されてきたとの見方をより支持し易い。

（2）サイバー任務部隊（CMTs）の新編：弥縫策を通じた「二重の統合」の追求

ただし、特に 2018 年以降、蘭国防省が現行法制上の制約を前提とした弥縫策の採用により、OCC の即応性確保に向けた「二重の統合」の強化を試みてきたことは特筆に値する。そのなかでも重要な施策は、2018 年の「国防サイバー戦略 2018」（以

72 Liza van Lonkhuyzen and Kees Versteegh, "Het Cyberleger Kan en Mag Nog Weing," *NRC Handelsblad*, December 18, 2018, https://www.nrc.nl/nieuws/2018/12/18/het-cyberleger-is-er-wel-maar-mag-weinig-a3099254; Smeets, *No Shortcuts*, p. 68.

73 Max Smeets, "The Challenges of Military Adaptation to the Cyber domain: a Case Study of the Netherlands," *Small Wars & Insurgencies*, vol. 34, no. 7（July 2023）, pp. 1349–1352; Alexander Claver, "Governance of Cyber Warfare in the Netherlands: An Exploratory Investigation," *The International Journal of Intelligence, Security, and Public Affairs*, vol. 20, no. 2 (May 2018), pp. 167–169.

74 Claver, "Governance of Cyber Warfare," pp. 167–169.

75 Sergei Boeke, "Hackers, Wiz kids, en Offensieve Cyberoperaties: Uitdagingen voor het Defensie Cyber Commando," *Atlantisch Perspectief*, vol. 42, no. 5 (2018), pp. 28–30.

76 Smeets, *No Shortcuts*, pp. 68–69, 204; Smeets, "The Challenges of Military Adaptation," pp. 1345–1347.

下：DCS2018）が掲げたサイバー任務部隊（CMTs：Cyber Mission Teams）の新編である[77]。DCS2018によれば、CMTsはDCCとMIVD双方の出向者を軸とした共同部隊であり、必要に応じて在来戦力等の運用を担う作戦コマンドの要員等も包摂しつつ、蘭軍展開時には参謀総長の隷下に置かれたDCCの権限に沿ってOCOを遂行する。DCS2018はCMTsの編制経緯について、（PB）OCCの整備/運用におけるインテリジェンスと軍事作戦の知見・技能の不可分性に触れながら、CMTsが他国での先進事例に倣う形でデザインされたものである点に言及している[78]。

そしてDCS2018の刊行から約4年後、2022年7月に公表された同国の2022年版の国防白書（以下：DWP2022）[79]と、その2か月後の同年9月、同国の軍事雑誌に対してMIVD職員2名が匿名で寄稿した論文（以下：CMTs論文）[80]も、蘭軍でのCMTsを梃としたOCCの整備/運用の方針につき、次の2点の重要な示唆を含む。

第1には、自由民主主義国家としてのオランダによるOCCの整備/運用の所要への言及である。特にCMTs論文は、MIVD要員が2010年代に同国のCiv-INTELである総合情報保安局（AIVD）との共同部隊で実施してきたCNEの教訓を振り返り、本稿が扱うPBOCCにあたる能力整備/運用の課題に言及する。そこには例えば、攻撃手法の標的毎の個別性や耐用期間の一時性の問題や、標的への侵入検知で生じる政治的リスクゆえの、攻撃手法の秘匿を含むOPSECの維持の要請等が含まれる。そのうえでCNEとCNAは、侵入後の標的環境や運用する攻撃ツールやインフラの管理の暗黙知を要するため、実務上は異なる組織間の能力移転が困難であり、CNAの遂行にはCNEの段階から運用の関係当事者が緊密に連携する必要性を説く[81]。

第2に、DWP2022とCMTs論文は共に、CMTsが、本稿の示す「二重の統合」の機能を促すとの認識を示している。例えば「第1の統合」について、CMTs論文ではDCCとMIVDの双方の要員による平素からの緊密な協働は、有事にCHOD指揮下で展開される軍事作戦での所要の早期の吸収は、OCCの蘭軍全体の作戦計画に対する統合を進める点に言及がある[82]。またDWP2022も、マルチドメイン作戦を支えるOCCの意義に触れ[83]、その上でMIVDとの緊密な協力を前提としたCMTsが「デジタ

77 NLMOD, *Defence Cyber Strategy 2018: Investing in Cyber Striking Power for the Netherlands*, November 12, 2018, p. 13.
78 Ibid.
79 NLMOD, *A Stronger Netherlands, A Safer Europe: Investing in a Robust NATO and EU*, 2022 Defence White Paper, July 19, 2022.
80 Anonymous, “All about access: Insights from NLD DISS Cyber Operations and Their Implications for Digital Striking Power,” *Militaire Spectator*, vol. 101, no. 9 (September 2022), pp. 24–35.
81 Ibid., pp. 25–30.
82 Ibid., p. 33.
83 NLMOD, *A Stronger Netherlands*, pp. 42–43.

ル打撃力（digital striking power）」の開発や、更には CMTs や各作戦司令部との協力を通じた「作戦構想に対する各種サイバー作戦の統合」を進めると記す[84]。また CMTs 論文は「第 2 の統合」について、CMTs が DCC と MIVD の両機関の法的権限を組み合わせることで OCO のターゲティング・サイクルのなかで必要な法的権限の欠缺の問題を緩和し、同時に平素からの両機関要員の協働が双方の知見や組織文化のギャップの克服にも寄与することを強調する[85]。

（3）陸軍 CEMA 中隊（NLA-CEMAC）による EBOCC の模索

上述の CMTs と並んで、オランダ軍隷下の MCF による OCC の整備 / 運用の事例として注目に値するのは、2021 年 7 月、蘭陸軍の指揮統制支援コマンド（C2OstCo）の隷下部隊として新編された NLA-CEMAC である[86]。この NLA-CEMAC をめぐっては、組織の新編経緯や能力整備 / 運用の指針について、少なくとも次の 2 つの論点を指摘できる。

第 1 の論点は、目指されるべき能力整備 / 運用の方向性と組織の機能である。この点、NLA-CEMAC は、陸上作戦の支援を主眼としつつ、戦術級の能力としての EBOCC の整備 / 運用の基盤提供に特化する意向を示している。例えば同年 7 月の蘭国防省の公式発表は、NLA-CEMAC の編制上の地位に触れつつ、NLA-CEMAC を「国家級のサイバー能力を持つ DCC の存在を前提に、既存の取組を前進させるもの」であり、これを「既存の戦力を補完するため、陸上作戦におけるデジタル及び無線領域での作戦の展開」を担うと説明し、NLA-CEMAC の取組の例示として「（権限が付与された場合の）敵対者のコンピュータのハッキング、電話の通話傍受、敵対者の通信の妨害」を挙げる[87]。

上記の国防省の公式発表にあるように、NLA-CEMAC の任務には陸上作戦の文脈における OCO の遂行が含まれる。この OCO が想定する具体的な技巧は、同時期に刊行された蘭陸軍の特集記事も一定の示唆を提供する。同記事は、同年 7 月の NLA-CEMAC の新編の意義を、過去の陸軍の演習での CEMA の実証実験にも触れながら説明する。そこでは、第 17 機動歩兵大隊と共に展開された戦術情報機動チーム（TIMT：Tactische Informatie Manoeuvre Team）が、部隊展開地域で（敵対者の）個人用 PC

84 Ibid., p. 52.
85 Anonymous, “All about access,” p. 34.
86 Ibid, pp. 24–25.
87 NLMOD, “Landmacht Versterkt met Cyber- en Elektromagnetische Capaciteit, ” July 9, 2021, https://www.defensie.nl/actueel/nieuws/2021/07/09/landmacht-versterkt-met-cyber--en-elektromagnetische-capaciteit#:~:text=De%20Koninklijke%20Landmacht%20is%20versterkt,（via%20de%20lucht）%20ondersteunen.

端末やルーター等の情報通信機器を標的としたISR活動を実施した事例や、このISR活動の成果を踏まえたより攻勢的なCEMAの選択肢として、例えば歩兵部隊の標的の建造物への接近に伴い、敵対者の運用する監視カメラの機能の掌握といった取組が列挙されている[88]。

ここまで見た限り、NLA-CEMACは支援対象の陸上部隊とセットで前線に展開され、敵対者のC4ISRを阻害するEBOCCの整備/運用の基盤を担う機能が想定されている可能性が高い。この点は2010年代後半の蘭軍が、米陸軍との政策対話[89]やオランダのシンクタンクへの委託研究事業[90]を通じ、同種の運用構想を有する米陸軍におけるCEMAの先進事例の吸収を試みてきた形跡からも傍証される[91]。

第2の論点は、NLA-CEMACがEBOCCの整備/運用を目指すことの「二重の統合仮説」への含意である。本稿第2節で触れた通り、EBOCCの整備/運用の所要は、アセットや専従部隊の事前配備や権限委任等を通じた前線における運用の自己完結性にある。同時に、蘭国防省の説明によれば、NLA-CEMACはDCCの代替ではなく補完の役割を担う。この点を踏まえてNLA-CEMACの動向を「第1の統合」と「第2の統合」の枠組で捉えた場合、NLA-CEMACは前線の在来戦力に対する戦力増幅機能を高め、専ら戦術レベルでの「第1の統合」を促す試みとも解釈できる。また「第2の統合」につき、DCCではターゲティングとBDAでのMIVDの支援が強調されてきたが、NLA-CEMACが目指すCEMAは、運用に要するISR活動を部隊展開地域で完結させる発想も垣間見える。これを、PBOCCではINTELの組織的支援を要する機能を、EBOCCでは戦術/作戦単位の部隊自体に内製化したものと捉えれば、「第2の統合」の作用の部分的発露とも解釈しうる。

ただし、前段の記述は先行研究で指摘されてきたEBOCCの整備/運用の所要と、NLA-CEMACをめぐる断片的な史資料に基づく仮説に留まる。この点で、蘭国防省の公式発表が述べる通りNLA-CEMACとDCCは能力の整備/運用の様式の分業に根差した相補的なものか、あるいは、限られた予算・人員の配分や運用局面における両者の標的の重複等を契機とした競合性を備えるものか否かといった論点は、将来の

88 André Twigt, “CEMA-compagnie: Digitale Draadloze Oorlogsvoering,” *Landmacht*, vol.6, no.5, July 2021, https://magazines.defensie.nl/landmacht/2021/06/05_cde-rubriek.

89 例えば2017年、DCCは米陸軍サイバーコマンドから、戦術/作戦単位の前線部隊に対するOCCによる支援についての知見の共有を受けている。次を参照。Steven P Stover “Partnership between Dutch and Army Cyber Brigade Benefits Both Nations,” U.S. Army, May 23, 2017.

90 次を参照。Louk Faesen et.al, *Naar een Cybercapaciteitenportfolio voor de Koninklijke Landmacht*, HCSS Security Series（Hague：The Hague Center for Strategic Studies, January 2021）.

91 例えばステファン・ソエサント（Stefan Soesanto）は、前掲注での委託研究事業の分析と提言内容を紐解いたうえで、「（米陸軍由来の）CEMAの蘭陸軍の文脈への変換を目指したもの」と評価する。次を参照。Soesanto, *A Digital Army*, pp. 19–20.

DCC/CMTs と NLA-CEMAC の双方の展開実績の情報公開を通じた後世の検証を待つことになるだろう。

おわりに

本稿での米蘭の比較事例研究の結果は、以下の表 2 の通り整理できる。全体的に事例研究の結果は、本稿の掲げた「二重の統合仮説」の内容を支持しつつも、2018 年以前の DCC のように、必ずしも能力整備 / 運用の合理性からは組織編制を説明しえないケースが存在するほか、NLA-CEMAC の事例は、EBOCC の整備 / 運用をめぐるムーアの議論の想定と合致する一方、「第 2 の統合」の機能をめぐっては議論の余地を残すものとなった。

表 2　本稿における米蘭の MCF をめぐる比較事例研究の結果の要約

観察事例	観察事例の仮説に対する支持度	事例の含意の要約
事例① 米 JTF-ARES （USCYBERCOM 隷下）	（＋＋＋） 強い支持	JTF-ARES は OCO の各戦闘軍 / 同盟国との統合 / 連合作戦への組込や軍事的要請と政治的要請の衝突の調整を担保。またターゲティングや BDA の局面における IC からの運用情報支援も調達。「二重の統合仮説」を支持する典型的事例。
事例② 蘭 DCC （蘭参謀総長隷下）	2018 年以前 （＋） 限定的な支持 （含意に解釈の余地）	DCS2012 以来、「二重の統合仮説」と合致した能力整備 / 運用の指針は示すが、必ずしも指針を具体化するために必要となる合理的な組織・制度設計はなされず。DCC の編制をめぐる国内政治要因等の影響を否定できず。
	2018 年以降 （＋＋＋） 強い支持	2018 年以降の CMTs 新編による DCC と MIVD の連携強化の動向は、DCS2018、DWP2022、CMTs 論文の記載と照らしても、PBOCC の即応性確保に向けた「二重の統合仮説」の機序を支持。
事例③ 蘭 NLA-CEMAC （蘭陸軍 C2OstCo 隷下）	（＋） 限定的な支持 （含意に解釈の余地）	NLA-CEMAC の取組は EBOCC の整備 / 運用の所要を反映し、陸軍による戦術レベルでの「二重の統合」の試みとも解釈は可能。ただし CMTs を含めた DCC の取組との相互作用は、現時点では観測困難。

（出所）本稿第 4 節・第 5 節における事例研究の結果に基づき、筆者作成

以上を踏まえた本稿の含意は、第1に、古典的な軍事力とインテリジェンスをめぐる学術研究が体系化してきた組織・制度論上の示唆が、国家のサイバー攻撃をめぐる学術研究の基盤としても有用と示した点にある。事例研究が示すように、自由民主主義国のMCFは、その戦略目標や法令遵守の要請ゆえにOCCの整備/運用の自由度を制約され易く、同時に能力の作戦計画への統合から運用情報支援の制度化に至るまで、様々な課題を能力の即応性の確保・維持に向けて克服する必要が生ずる。こうした現象の歴史的・理論的な連続性を捉える視座は、しばしば「新領域」として革新性が強調され易いサイバー安全保障の政策論議を相対化しつつ、より実態に即した各国の能力評価を可能とする[92]。

この点と関連した第2の含意は、各国政府のサイバー安全保障体制のガバナンスをめぐる学術・政策的論争への貢献にある。本稿の結論はサイバー空間の課題に対処する国家のインテリジェンス機能が、INTELという組織単体では完結せず、既存のINTELと他機関の間での運用情報支援の制度化を通じて具体化される側面を示した。同時に、JTF-ARESやCMTsのような運用情報支援の制度化に向けた「二重の統合」を試みた組織モデルは、米国では例えば麻薬取引阻止のための多国間海上法執行活動[93]でも前例がある。本稿が提示した議論は、こうした隣接事例を含む比較研究を行う礎石としての意義も有する。

最後に、本稿の結論の内在的制約と今後の研究課題に触れたい。本稿の「二重の統合仮説」は、米蘭2か国の範囲では概ね支持されたにせよ、必ずしも全ての民主主義国におけるMCFの発展モデルの一般的な説明をなしうるものではない。現実には各国のMCFはOCCの整備/運用のみを目指す訳ではなく、2018年までのDCCの事例が示す通り、国内政治過程や既存法制上の制約を含む経路依存的な要因により、各国のMCFは必ずしも軍事的合理性を反映しない形の発展も遂げうるからである。この点、今後は非西欧圏も含む多様な民主主義国のMCFの発展モデルの探索的研究と並行して、国・地域毎の異なるMCFの発展モデルを導く潜在的要因や機序を明らかにする作業が求められよう。

（防衛研究所）

92 次を参照。Smeets, “A Matter of Time,” pp. 26–27, 51–52; Moore, *Offensive Cyber*, p. 116.
93 次を参照。Evan Musing and Christopher J. Lamb, *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success*,（Washington DC: National Defense University Press, 2011）.