NIDS 防衛研究所
The National Institute for Defense Studies

政策シミュレーションにおける領域横断的事態と将来戦：シュリーバー・ウォーゲーム 2012・インターナショナルの再検討

政策シミュレーション室長　阿久津　博康

NIDSコメンタリー
第 178 号　2021 年 7 月 6 日

はじめに

領域横断的（クロスドメイン）事態への対応は、日本を始め今や多くの諸国にとって喫緊の安全保障政策上の課題となっているが、そうした事態は概念的にも実相としても極めて多様であり、容易に整理できるものではない。実際、米軍では多領域（＝マルチドメイン）という概念と領域横断という概念が併用されている。また、領域（ドメイン）についても、かつては宇宙・サイバー領域という括りが一般的であったが、現在ではこれに電磁波領域が新領域として加わっており、日本では「ウサデン」というジャーゴンが聞かれるような状況である。こうした概念的拡張の背景には、実際に生起した事案の存在があることは容易に想像し得る。しかし、こうした実際に生起した事例の影響とともに、特に欧米ではウォーゲーミングの役割が大きいことも看過すべきではない。何故なら、そうした実例を基に、ウォーゲーミングを通じてさらなる様々なシナリオが検討され、ウォーゲーミングの成果が諸計画に何らかの形で反映されるからである。

そこで、本稿では既に 10 年以上前から宇宙・サイバー領域作戦に関するウォーゲーミングを行ってきた米空軍のシュリーバー・ウォーゲーム（Schriever Wargame）について取り上げる。このウォーゲームを振り返ることで、米軍における初期の「マルチドメイン」作戦の捉え方のみならず、米軍が過去にイメージしていた将来戦の姿の一端を知ることにもつながり、日本にとっても参考となると期待できるからである。同ウォーゲームは 2018 年に防衛省・自衛隊等の日本の政府機関が初参加したことで注目されたが、基本的には通常の米軍のウォーゲームと同様に非公開でありその全貌は明らかにされない。同ウォーゲームに関する詳細な報告の中で、これまで唯一公開されているものは、「シュリーバー・ウォーゲーム 2012・インターナショナル（以下、SW2012I と表記）」報告のみである。よって、本稿は同報告を中心に紹介する。

シュリーバー・ウォーゲームとは

シュリーバー・ウォーゲーム（以下、SW と表記）は、米軍宇宙司令部が主催する宇宙をテーマとした年次のメガ・ゲーム（数百人単位のゲーム）であり、2001 年に開始した。宇宙にサイバー領域が加わった宇宙・サイバーのマルチドメイン・ゲームが本格的に始まったのは 2010 年である[1]。毎年 SW が開催される前後に簡単な紹介が報じられるが、これまで包括的な報告書が公開されたのは、先に述べたように 2012 年のゲームのみである。同年のゲームは、NATO 加盟諸国及び豪州が参加した。軍民約 270 名の専門家、30 以上の機関が参加した[2]。

さて、SW2012I の目的は 2 つある。1 つは、多国間協力における指揮系統の在り方の模索であり、2 つ目は宇宙空間での事態対処の共有ドクトリン・部隊行動基準の在り方の模索であった。また、準備については、前

[1] 勿論、2009 年以前のゲームでもサイバー及び宇宙の連関は扱われていたが、特に「宇宙・サイバー」に焦点を当てた演習が開始された 2010 年以降と見られる。

[2] SW2012I の報告書 *Schriever Wargame 2012 International* は変革連合軍司令官（SACT）により作成され発出された。全文は次のウェブサイトから入手可能である。
https://www.act.nato.int/images/stories/events/2012/sw12i/sw12i_report.pdf

年の 2011 年より宇宙及び法律専門家を中心とした部隊行動基準及び戦略文書に関する研究、作戦に関する資料等に関するワークショップを通じて行われた。こうしたワークショップを通じて、概念開発や NATO 諸国のアセットの調整等が可能となる。次に、チーム構成については、青チームは NATO 諸国であり、これにはカナダ、デンマーク、フランス、ドイツ、イタリア、オランダ、トルコ、英国、米国が含まれている。他方、赤チームは、テロリスト、海賊、サードパーティの支援国という構成である。

初期設定及びゲーム展開の概要

初期の状況設定は概ね次のとおりである。即ち、

-舞台は 2023 年のアフリカの角。国連安保理決議に基づき、NATO は人道支援のための周辺海域の通航の安全を確保しようとしている。NATO 軍は同地域で海賊対処作戦を展開中

-同地域ではアル・シャバブが主要なテロの脅威となっており、商船に対して海賊行為に及ぶ

-アル・シャバブは闇市場及び第三国を通じて一定の宇宙・対抗宇宙（space-counter space）能力を有す

-旱魃と飢餓により多国間救難作戦の必要性が高揚

-北大西洋理事会（NAC）は国連決議に基づき戦略指針を作成

-NATO 諸国及び豪州は人道支援（HA）及び航行の自由（FON）確保のために派軍

上記を初期設定として、5 日間に渡って演習が実施された。日毎に複数のムーブが付与され、各ムーブは複数のイベントから成るシナリオとして提示された。以下は日毎の各ムーブにおける結果である。

1 日目（6 ムーブ）：1）エジプト及びブラジルの衛星が衝突、非静止・低軌道衛星システムの軌道にデブリクラウドが発生。2）無関係の事象として、一連の国連決議を支持してこなかったある国家が、衛星打ち上げ準備を継続。但し燃料未注入。3）商用衛星画像提供業者によれば、アル・シャバブのフロント会社を含む複数の者からの画像需要が高まっている由。4）NATO 軍は GPS 及び通信ジャミングを散発的に受ける。5）ドイツのユーシンゲン衛星地上局で電力停止、バックアップ給電も不可となる。6）第 4 タスクグループが海賊攻撃を阻止、海賊をソマリアのキスマーヨ港まで追跡

2 日目（4 ムーブ：1）通信・GPS ジャミングが激しくなるも、NATO 軍の遮断措置によりその影響は希薄。2）イリジウム 2 衛星が先のエジプト・ブラジル衛星衝突で生じたデブリと衝突。3）フランス、ドイツ、そしてイタリアにある地上局がサイバー及び破壊活動を通じて攻撃を受ける。4）アル・シャバブの工作員がジブチに 2 発の Club-K ミサイルを発射。1 発目は失敗し海中弾着、2 発目はパトリオットにより迎撃される

3 日目（5 ムーブ）：1）能力格差を縮小すべく、イタリア及びオランダは作戦支援のために小型（マイクロ）衛星を打ち上げる。2）宇宙データ協会（SDA）は、同協会の宇宙状況認識（SSA）能力に対するサイバー攻撃が疑われると報告。3）操縦操作に狂いが生じると、対地静止軌道（GEO: Geosynchronous Earth Orbit）にあるオランダの衛星が問題に直面。4）諸国は NATO と協力してサイバー防衛について調整。5）アル・シャバブ及び海賊が共謀してジブチにある米軍基地に攻撃を行い、その結果重要な地上通信基地局及び光ファイバーケーブルが破壊

4 日目（4 ムーブ）：1）統合軍（JFC）は NATO 欧州連合軍最高司令部（SHAPE）及び各国と調整してジブチへの攻撃で喪失した能力を代替した。2）イタリアの小型衛星に通信障害が生じる。こうした問題は作戦を支援している他の複数の小型衛星の作戦に影響。3）フランス及び米国の特殊部隊が多国間救難活動従事者（multinational relief effort workers）が直面している問題に対処。しかし、暗闇と“戦場の霧”の中、通信・GPS ジャミングも相俟って、ケニア軍との味方同士の攻撃という事案が発生。4）非協力国の衛星が打ち上げ後 5 分に失敗、ロケットは遠方の豪州に着弾するも人的・財産的被害なし。

5 日目（最終日）（4 ムーブ）：1）法執行措置としてのコンピュータネットワーク搾取により、複数の国家でアル・シャバブの資金及びサイバー支援を遮断。2）青チームによる消極的措置により GPS 及び通信ジャミン

グの影響の殆どが拒否される。3）青チームによる積極的措置により GPS 及び通信ジャミングの発信源が除去され始める。4）アル・シャバブが残存するインフラ、財産、人員、資金及び資源を保全すべく地下に潜行

以上の展開を一瞥するに、海上での対テロ作戦が進行する中、宇宙及びサイバー次元での事態が連続的に発生、ジャミングを中心とした電磁波次元での事態が宇宙アセット及び活動に影響を及ぼし、“戦場の霧”による状況認識錯乱のため味方同士の攻撃も生ずるという、いわばクロスドメイン事態で想定される事象のオンパレードのような様相を呈している。上記には記載していないが、衛星基地局の職員がテロリストに殺害されるという想定もある。また、ゲームを青チームに有利な形で終息させるためか、最終日では赤チームによる青チームに対する行動が失敗するという結末になっている。但し、赤チームのテロ組織は一定の戦力を温存したまま潜伏する。このように、将来の危機を予期させる形でゲームは終了している。

ゲームで得られた知見及び教訓

ゲームで得られた知見及び今後考慮すべき点としては、例えば以下のようなものが提示されている。

-NATO 及び協力国の情報共有の制度的仕組みの必要性

-NATO 及び産業界との協働・調整ドクトリン開発の必要性

-宇宙・サイバー空間での効果的かつレジリエントな作戦が可能となる連合軍事力の構築

-宇宙アセット（能力）の十分なレジリエンス及び防護

他方、教訓については、ここでは 2 つの主要な教訓を紹介したい。第 1 に、NATO の作戦を支援する宇宙諸能力（アセット）が脆弱である。端末から端末までの宇宙システムの安全は地上から衛星まで全ての面にとって必要である。今回のゲームでは、アル・シャバブが宇宙システムへのアクセス拒否を試みた結果、NATO の地上での作戦が妨害されてしまった。結局、青チームは地上で苦しめられる一方、統合作戦地域（JOA: Joint Operating Area）外で宇宙支援が妨害されることとなった。アル・シャバブは具体的に以下のような多様な作戦を展開し NATO 作戦を動揺させた。

-フランス地上局の職員に対して毒を使用⇒衛星データ・情報プロセス妨害

-サイバー攻撃及び燃料汚染を通じてドイツ及びイタリアの地上局への送電に対する破壊工作

-SCADA（Supervisory Control and Data Acquisition）を通じてフランス、ドイツ、イタリア、そしてトルコの地上局に対するサイバー攻撃

-サイバー攻撃で SDA（Space Data Agency）のデータベースへのアクセスを拒否した後、データを汚染してから SDA のクライアントに誤った衝突警告メッセージを送信

-デブリ軽減衛星の遠隔測定・追跡・遠隔制御（TTC: Telemetry, Tracking, and Control）へのハッキング

-内部のシンパを利用して商用軌道上衛星サービスソルーション（COSSS: Commercial On-Orbit Satellite Servicing Solutions）を汚染

-デブリを創出する衝突等による混乱の惹起

-ハッカーを雇って断続的な不法行為を通じての混乱の惹起

-海賊、民兵、地元住民による通信・GPS ジャミング

-戦域内の地上基地局及びファイバー光ケーブルに対する物理的攻撃

第 2 に、そしてゲームが示唆する最大の教訓として、サイバー対応の優先性が挙げられる。即ち、「サイバー能力は宇宙能力なくして戦力となり得るが、宇宙能力はサイバー能力なくしては戦力にはなり得ない」（Cyber can fight without Space, but Space cannot fight without Cyber）ということである[3]。純然たる宇宙作戦としての NATO 作戦は未だになく、実際の作戦は常に宇宙と陸・空・海との関連で実施されてきた。今回、宇

[3] SW2012I の報告書、p. 36

宙・サイバーとの関連という観点でゲームを行なったところ、上記気づきを得るに至った由である。即ち、SW2012I では、今やサイバー空間を通じて多くのものがさらに繋がるようになっている世界において、ドメインとしてのサイバー空間は全ての作戦ドメインの中で最も重要な要素として認識されるようになった、ということである。

おわりに

SW2012I で想定される主戦場はあくまでも地上または海上であり、サイバー戦が地上または海上に影響を与え、それを通じて宇宙での監視活動や軍事作戦が影響を受ける、という展開となっている。ここに、マルチドメインまたはクロスドメイン型ウォーゲームの初期のひな形が見て取れる。また、同ゲームには電磁波領域という概念は明示的には表れていないが、アップリンク・ジャミングも当然想定されており、その意味で初期の宇宙・サイバードメインゲームとして有益な参考事例となろう。しかし、同ゲームから導出された「サイバーが宇宙に優先される」という教訓は、現在ではやや単純すぎるという批判は免れない。何故なら、2020 年代のマルチドメインまたはクロスドメインの実相は、遥かに複雑なものだからである。特に、主戦場が地上または海上であるかどうかは議論が分かれるところであろう。地上や海上での武力衝突はなくとも、サイバー・宇宙ドメインで激しいバトルが生じる場合もあるからである。人的介在や可視性が比較的低いドメインであるサイバー戦では、エスカレーションが激化する可能性は高い。実際、日々刻々と何らかのサイバー戦が繰り広げられている現在、その程度たるや想像を絶するものとなるかもしれない。このことは、ロシアがウクライナで展開したハイブリッド戦を想起すれば容易に首肯できよう。宇宙についても、キラー衛星になり得る衛星数も急増しつつある。宇宙が実質的な主戦場となる可能性も、容易に否定はできないであろう。

なお、本稿では詳細に取り上げなかったが、SW2012I では図 1 のような NATO における宇宙・サイバーに関する危機管理及び指揮命令の仮想の実験装置を設定し、その検証が行われた。図 1 で示されている各所の名称は現在一部変更されているが、こうした架空の危機管理・意思決定装置を予め想定し、その機能をゲームで検証しようというアプローチは、日本で政策シミュレーションを行う場合も大いに参考となるものである。もし日米同盟や米国を中心としたインド太平洋の同盟システムにおいて類似の意志決定実験装置を想定するとすれば、どのようなものが考えられるであろうか。

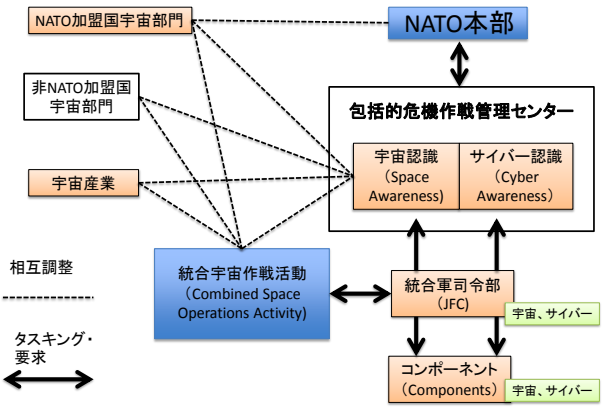

図 1　包括的宇宙・サイバー危機管理組織の模式図（例）
（出所：SW2012I の報告書、p. 36 を基に筆者作成）

既にウォーゲーミング先進諸国ではサイバー・宇宙ドメインをめぐるウォーゲーミングが積極的に構想され、具体的なゲームが試みられている。将来戦研究が一層重要となる中、政策シミュレーションについても様々な構想をめぐらす必要がある。

プロフィール profile

政策シミュレーション室長

阿久津　博康

専門分野：政策シミュレーション、朝鮮半島の政治・軍事

防衛研究所企画部企画調整課
直　通：03-3260-3011
代　表：03-3268-3111（内線 29177）
ＦＡＸ　：03-3260-3034
※ 防衛研究所ウェブサイト：http://www.nids.mod.go.jp/