ロシアの2025年に向けた電子戦能力
電磁波スペクトラムにおけるNATOの挑戦
㊦

2017年9月
ロジャー・N・マクダーモット　　訳／木村　初夫
エストニア共和国　国際国防安全保障センター　　株式会社エヌ・エス・アール　代表取締役
井手　達夫
海上自衛隊幹部学校　未来戦研究所　二等海佐

3.1.3　クリミア、ドンバスへ－見えない支援

シリアにおけるロシアの作戦とはまったく対照的に、クリミアの占領とドンバスの戦争は、大規模な電子戦使用に大きく依存しており、またウクライナ南東部での紛争は、電子戦システムにおけるロシアの実験のテストベッドとして役立った。ウクライナ軍のクリミア喪失の実績は、他で十分詳細に評価され、概説されている[88]。ロシアのドンバス介入では、電子戦が大きな役割を果たし、より少数の軍人がウクライナ軍に対して畏怖の念を起こさせている挑戦に注目することが重要である[89]。しかし、クリミア(戦闘を伴わない)の占領作戦と、その後のウクライナ南東部の紛争を通じたロシアの電子対策の使用は、代理部隊の支援と比較的小さな部隊を用いたウクライナの大規模な地域の不安定化を成功させる重要な要因として誤解され続けている。

マイケル・コフマン他は、ロシアのドンバスにおける作戦に先駆けた西側の事前占領を、全体を通じて「ハイブリッド戦争」と呼ぶのは最低限でも短絡的だとしている。

> *何人かの西側のアナリストは、ウクライナ東部における戦争をハイブリッド戦争として特徴付けている。しかし、この観点は正しくない。むしろ、2月から8月までの紛争は、政治戦、非正規戦、ハイブリッド戦争、および通常戦争の4種類の戦争を繰り返した。ロシア連邦軍参*

88) See Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva and Jenny Oberholtzer, Lessons from Russia's Operations in Crimea and Eastern Ukraine (Santa Monica, CA : RAND, 2017) : 22-5, 67-70.

89) Author interviews with Ukrainian EW experts, Kyiv, May 2017.

謀本部の考え方にそのような教義や方法が存在するという議論があったにもかかわらず、ロシアがハイブリッド戦争を行うことを意図した兆候はない。ほとんどウクライナでの紛争の初期の日については、参謀本部の監督と関与を示していない。ロシアの戦術選択は教義主義的なものではなく、むしろウクライナの抵抗に対する一連の場当たり的な対応であった[90]。

確かに、西側の政策立案者は、クリミアで展開された事案のように軍事力に頼ったキエフが示した「自制」を素早く賞賛した。その見方はNATO分析官と著者との私的な会話においてしばしば共有されている[91]。それにもかかわらず、特殊作戦部隊と支援部隊を含むクリミアでのロシアの軍隊の投入に関する詳細についての注意深い言及は、実際にロシアの電子戦の役割がどのように重要であるかを明らかにしている。

高度に訓練されたロシアのさまざまな軍事専門要員がウクライナの軍事基地周辺の半島を横断し展開されたため、電子対策はウクライナ軍がウクライナ本土と通信するのを遮断するために使用された。ウクライナの軍事施設は固定および有線の通信手段に依存していたので、その指揮統制を断ち切るため、地元の軍人の利点を活用し、ロシアのスペツェナズ（Spetsnaz）部隊がこれらの回線を素早く切断し、クリミアのウクライナ軍事施設を隔離することを可能にした。たとえば、2014年3月11日までに、より多くの地上部隊がケルチ（Kerch）海峡を横断してクリミアに移動し、その中にはLeer-2、Lorandit、およびInfauna電子戦システムが見られた[92]。

対照的に、ドンバスの場合、ロシアの大多数の電子戦システム（**表1**参照）が現れ、ウクライナとの穴だらけの国境を横断して移動し、これらの電子戦システムを実験する機会を提供した。たとえば、2017年5月13日に、欧州安全保障協力機構（OSCE）特別監視団（SMM）は、ロシア製のOrlan-10 UAVがマキイフカ（Makiivka）（ドネツク［Donetsk］）の北東12km）からドネツク市に向かって飛行していることを観測した。頻繁に見られたOrlan-10は、Leer-3電子戦システムの一部として機能する[93]。しかし、可能な限り、作戦や独立主義者のためにロシアの電子戦支援において持続する役割を果たす多くのシステムが特定された。これらは、ドンバスをロシア軍の基本的な実験場として使用するための広範な取り組みの一部であるとみられる。

すでに述べたように、電子戦アセットと専門要員は、ロシアの陸軍内で機動ユニットとして運用している。ドンバスの課題の一部は、ロシアの電子戦専門家の中には、独立主義者組織に組み込ま

90) Kofman et al, Lessons from Russia's Operations: 69.
91) Author research interviews in Mons, December 2015 and Rome, September 2014.
92) Kolesova and Nasenkova, Radioelektronnaya bor'ba, op. cit.: 229.
93) "Latest from the OSCE Special Monitoring Mission to Ukraine (SMM), based on information received as of 19: 30, 14 May 2017", OSCE Special Monitoring Mission to Ukraine, last modified May 15, 2017, accessed July 10, 2017, http://www.osce.org/special-monitoring-mission-to-ukraine/317386. Orlan-10 UAVs have also been shot down by the Ukrainian Armed Forces during the conflict in the Donbas.

表１　ドンバスに配備されているロシア電子戦システム

電子戦システム	機能
RB-341V Leer- 3	GSM 通信電波妨害
RB-301B Borisoglebsk- 2	自動電波妨害システム（探知、方向探知、HF／VHF 無線通信の分析と制圧）。R-330KMV 指揮所と妨害局を含む。
R-934UM	電波妨害局（探知、方向探知、VHF／UHF 無線通信の分析と制圧）。R-330 M1P Diabazol 自動電波妨害システムの一部
R-330Zh Zhitel	SATCOM／GPS／GSM 電波妨害局（探知、方向探知、UHF 無線信号の分析と制圧）。R-330M1P Diabazol 自動電波妨害システムの一部
Shipovnik-Aero	UAV 傍受システム
Torn	電波妨害局（仕様不明－現在サービス停止中）
Rtut-BM	電波近接信管妨害局（近接信管使用弾頭からの人員と装備の防護）
RB-636AM2 Svet-KU	電波監視およびさまざまな電波放射源追跡
R-318T Taran	COMINT システム。指揮所と HF／VHF／UHF 距離で運用する局
MKTK-1A Djudist	無線制御・情報防護システム（探知、方向探知、および無線信号の分析）。電波管制を支援するように意図されている。

れている可能性もあるが、しばしば間接的に地元の代理部隊の訓練と使用を通じてこの支援を提供することであった。これにより、ロシア軍は広範な異なる種類の作戦において電子戦アセットを利用する上で極めて重要な経験を得て、またこれを独自の作戦環境のニーズに適合するようカスタマイズすることができた。より直接的な介入にだけ、イロバイスク（Ilovaysk）とデバルツェボ（Debaltseve）の敵軍を一掃するために連合作戦を主導するロシア軍を必要とすることは、これがロシア軍による将来の正規作戦にどのように統合されるかについて与えられる洞察である[94]。「もっともらしい拒否権」の文脈では、ドンバスにおけるロシアの電子戦活動は必然的に秘密であり、評価することは困難である[95]。

電子戦はドンバスの紛争ですべての当事者によって使用された。独立主義側では、これは携帯電話信号を阻止することから軍事通信システムやレーダーを目標とする電波妨害に至るまで広範な電

94) Paul Robinson, “Explaining the Ukrainian Army’s Defeat in Donbass in 2014”, in J.L. Black and Michael Johns (eds), The Return of the Cold War : Ukraine, the West and Russia (London : Routledge, 2016) ; Roger N. McDermott, Brothers Disunited : Russia’s Use of Military Power in Ukraine (Fort Leavenworth : Foreign Military Studies Office, 2015), https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/197162 (accessed July 10, 2017). Charles K. Bartles and Roger N. McDermott, “Russia’s Military Operation in Crimea : Road-Testing Rapid Reaction Capabilities”, Problems of Post-Communism Vol. 61, No. 6 (2014) : 46-63.

95) Bartles and McDermott, “Russia’s Military Operation in Crimea”.

子戦の作戦をカバーした。OSCE SMM は、OSCE Schiebel S-100 Camcopter UAV を目標とする電子攻撃の使用によって、頻繁にその作業を妨害された。すなわち、これらはクラッシュするか、自動帰還モードになった。紛争における電子戦の使用は、次のように分類することができる。

・コントローラまたは GPS 信号の電波妨害によってウクライナの UAS を目標にする電子戦
・火砲から臼砲の電子信管弾頭を破壊する電子対策
・敵の通信の混乱：地域の一部での通信システム機能停止
・指揮統制を目標にする：ロシアの電子戦アセットは、位置特定および目標とされる電磁波放射を検知する[96]。

紛争中、ウクライナ軍はロシア軍および代理部隊による電子戦の積極的な使用により、敵の電磁波環境での作戦を学んだ。これには、西側の軍隊の限られた訓練と情報提供、少数の単一回線地上航空システム (SINGGARS) の米国による提供が含まれていたが、無線網暗号化はウクライナの軍事作戦では普及していない。ロシアは確かにドンバスに運用中の電子戦システムと試運転中の新しい機器の両方を配備した[97]。さらに、ロシアの電子戦機器に関して、RB-341V の Leer- 3 電子戦車両と Borisoglebsk- 2 は巨大な姿を現した。しかし、目撃者によれば、これらは前線から離れ、ロシアの国境付近に巧妙に配置される傾向があった[98]。

ウクライナ参謀本部が電子戦の領域を秘密に指定しているため詳細は不明だが、オープンソースの報告と著者のインタビューでは、ドンバスのロシアの電子戦作戦の最も革新的な特徴を特定することができた。第一に、戦闘中に高度に機動性のある戦術電子戦集団を使用し、火力下での破壊を避けるために絶えず場所を変えた。すなわち、この方法の要素は初期の局地紛争で現れたが、ロシア参謀本部が転々と移動して作戦できる独立した戦術電子戦集団を展開する方法を考案したようである。第二に、ロシアの電子戦部隊は新しい電子戦アルゴリズムを実験した。しかし、主な革新は、作戦の支援に電子戦の非常に大規模な使用を置いていた。また、ロシア参謀本部は、新しい戦術の実験と自動化された移動体システムの有効性を非常に重視していたようである。すなわち、シリアでの作戦ではなく、この基本的な立場で、ロシア参謀本部が2017年初頭にロシア軍に新しい電子戦マニュアルを導入したとの兆候があった[99]。

96) Author interviews with members of the OSCE SMM, Kyiv, May 2017 ; interviews with NATO EW specialists, Washington DC, June 2017.
97) Author interviews with members of the OSCE SMM, Kyiv, May 2017 ; interviews with NATO EW specialists, Washington DC, June 2017.
98) Author interviews with members of the OSCE SMM, Kyiv, May 2017.
99) Author interviews with Ukrainian EW specialists, Kyiv, May 2017 ; " 'Dobyto v shakhte' : Na vooruzhenii terroristov LNR stoit rossiyskaya perenosnaya stantsiya razvedki 'Kredo-M1'. Foto" [" Mined from a mine" : weaponry of LNR terrorists includes a Russian mobile reconnaissance station Kredo-M1. A photo], Begemot, March 26, 2017, http://begemot.media/news/dobyto-v-shahte-na-vooruzhenii-terroristov-lnr-stoit-rossijskaya-perenosnaya-stantsiya-razvedki-kredo-m1-foto/ (accessed July 10, 2017).

3.1.4　行動中の電子戦－イロベイスクとデバルチェボ

ウクライナ紛争の２つの機会に、ロシアの部隊とその装備によって直接分離主義者を上陸させるために介入した。すなわち、それらの機会とは2014年８月のイロベイスクとミンスクⅡサミットの結果となる2015年１－２月のデバルチェボであった。これらは戦争に対する典型的な諸兵科連合アプローチによって特徴付けられ、それぞれの場合にロシアと代理部隊は局地的な勝利を迅速に確保した。しかし、各事例には、局地作戦の準備、実施、完了における電子戦アセットと電子戦の使用も含まれていた[100)]。

ドネツクから東へ25km に位置する戦略的に重要なイロベイスクの場合、一連の運動エネルギー的な接触は、プスコフ（Pskov）とクルスク（Kursk）のロシア軍によるウクライナ軍の包囲を速めた。すなわち、これはロシアの領土から紛争地域に移管された電子戦部隊を含む大隊戦術班、偵察および業務妨害班の展開を伴った[101)]。電子戦アセットも、前哨戦に先立って、確実な作戦の準備としてその地域に到着した。すなわち、これらは敵の通信を制圧するために使用された。

これらのシステムには、Leer-２複合装置、1L262E Rtut-BM、敵の情報・監視・偵察（ISR）を制圧するための Shipovnik-Aero、または Krasukha-２と Krasukha-４のような GPS 信号と UAV データリンクを妨害する局、および自動妨害複合装置 Borisoglebsk-２が含まれていた。ロシアの電子戦アセットは、戦術および作戦レベルでの無線通信の制圧、電磁波スペクトラム使用の特定による敵部隊の特定と位置特定、指揮統制の混乱、携帯電話ネットワークの遮断、心理戦の一環としての携帯電話ネットワークの遮断と偽情報の拡散の任務を課されていた[102)]。

これらの目標を達成するために、電子戦は作戦領域から同心円状に配置され、使用された。RB-531 B Infauna は、Rtut-BM、Leer-２および Lorandit 複合装置によって支援され、１～３ km の距離で運動エネルギー行動に対して再接近し、ウクライナ軍事通信を混乱させた。すなわち、これらは携帯電話（GSM）の使用に対して傍受し方向探知するものであった。通信回線外の15-30km の範囲で、ロシアの電子戦システムには、Leer-３、R-330ZH Zhitel、R-934UM、および自動化 Borisoglebsk-２が含まれていた。さらに通信回線から60～240km で、Shipovnik-Aero、Krasukha-２、および DRLOU A-50空中早期警戒機のような航空制圧システムが使用されていた。言い換えれば、これらの距離で、電子戦作戦のいくつかはロシア領土から実施されていた[103)]。

100）Author interviews with members of the OSCE SMM, Kyiv, May 2017.

101）Author interviews with Ukrainian EW specialists, Washington DC, June 2017.

102）Vyacheslav Gusarov, “Osobennosti organizatsii i vedeniya radioelektronnoy bor’by v boyakh za Ilovaysk. Analitika IS” [Peculiarities of battle order and conduct of electronic warfare in the battles for Ilovaysk. Analysis of IS], Informatsionnoye Soprotivleniye, December 5, 2016, http://sprotyv.info/ru/news/kiev/osobennosti-organizacii-i-vedeniya-radioelektronnoy-borby-v-boyah-za-ilovaysk-analitika (accessed July 10, 2017).

103）Gusarov, “Osobennosti organizatsii i vedeniya radioelektronnoy bor’by”.

イロベイスクにおけるロシアの電子戦使用の２つの特に重要な分野、すなわち心理戦を容易にするための砲撃のターゲティングと電子戦の補完的利用を強調しなければならない。ロシアの電子戦システムは、携帯電話を含む敵の通信伝送を探知し、砲撃を行うための目標情報を提供する。さらに、敵の携帯電話ネットワークを混乱させ、データを送信することによって、ウクライナの要員が電話でネガティブテキストメッセージを受信し、士気を損なうことを目的としたケースもあった[104]。このような心理戦と電子戦の統合は広範囲に及んでいないかもしれないが、確かに散発的に、またかなりの数の対テロ作戦要員の間で起こった[105]。

１月から２月にかけて、デバルチェボ周辺の地域では、戦略的に重要なルハーンシク（Luhansk）地域の輸送拠点の確保に重点を置いたロシア主導の作戦とともに、戦闘が急増した。ロシア軍と独立派部隊は、Minsk IIサミット周辺の外交にもかかわらず、デバルチェブを取ることによって、その地域を「整理する」必要性を見出した。イロベイスクのように、戦場を準備するのに先だってまた戦闘作戦中にロシアの電子戦システムが配備された。この機会の違いは電磁波スペクトラムを監視する任務を付与され、明らかにイロベイスクの初期に得られた経験を用いて包括的な技術的電子戦監視班を使用することであった。電子戦アセットは、ロシア軍によって方向探知／地理的位置特定のために配置され、他の機能との敵の通信を混乱させた。また、ロシア軍は、自動電波妨害器を使用した。電子戦作戦の全体計画は、無線調査／探知、妨害および情報分析の自動化されたサイクルを実現し、信号情報（SIGINT）と密接に連携してリアルタイムで情報を提供した。ロシアのグループは、再び電子戦システム（おそらくLeer-３）を使用して、心理戦が対テロ作戦要員を対象とすることを容易にした。すなわち、ウクライナ軍の兵士が士気を損なうことを目的としたテキストメッセージを受け取ったという多数の報告がある。同様に、高レベルの砲撃精度は、対テロ作戦要員間の通信における携帯電話の電磁波放射を特定することによって敵目標を特定し位置特定するための電子戦の適用の成功に起因するものであった[106]。

---

104) Author interviews with Ukrainian EW specialists, Kyiv, May 2017. It is unlikely that this could have been carried out on a wide scale, but rather it used deployed EW assets to target pockets of resistance. Equally, targeting enemy mobile phones in this way may also imply Russian access to sensitive Ukrainian military personnel details.

105) See “Electronic warfare by drone and SMS : How Russia-backed separatists use ‘pinpoint propaganda’ in the Donbas”, Atlantic Council’s Digital Forensic Research Lab, May 18, 2017, https://medium.com/dfrlab/electronic-warfare-by-drone-and-sms-7fec6aa7d696 (accessed July 10, 2017).

106) Vyacheslav Gusarov, “Taktika rossiyskikh grupp REB v boyakh za Debal’tsevo. Analitika IS” [Tactics of the Russian EW groups in the battles for Debaltsevo. Analysis of IS], Informatsionnoye Soprotivleniye, January 5, 2017, http://sprotyv.info/ru/news/kiev/taktika-rossiyskih-grupp-reb-v-boyah-za-debalcevo-analitika (accessed July 10, 2017) ; see also “Radioelektronnaya bor’ba rossiyskikh terroristicheskikh sil v nachal’noy faze voyennogo konflikta v Ukraine” [Electronic warfare by the Russian terrorist forces during the initial phase of the armed conflict in Ukraine], Informatsionnoye Soprotivleniye, September 20, 2016, http://sprotyv.info/ru/news/kiev/radioelektronnaya-borba-rossiyskih-terroristicheskih-sil-v-nachalnoy-faze-voennogo (accessed July 10, 2017).

ウクライナにおけるこれらの運動エネルギー作戦におけるロシアの電子戦の重要性は、将来の紛争においてそのようなアセットがどのように活用されるかについてのより深い洞察を提供する。軍事理論的レベルでは、コロリョフ（Korolyov）、コズリチン（Kozlitin）およびニキチン（Nikitin）がVoyennaya Myslの記事で主張しているように、ロシアの電子戦能力の開発は、これを将来の作戦の最前線に置くために指数関数的に進化している。これは、結局、純粋に戦闘支援の役割を果たすのではなく、軍種の武器としてその意味に値する。

> *これは、電子戦能力が軍種の武器であり、電子戦部隊と武器は戦闘行動を支援しないが、敵の部隊や武器の指揮統制を混乱させるための作戦上の任務を実現する場合、その戦闘行動に直接参加するという事実によるものである。それで、戦闘の使用における目標の方向付けは、敵の戦闘行動の実践的な指揮統制を混乱させることにある。さらに、その効率を評価することは、意思決定者に対する適時な情報支援を遅らせることによって現在の組織的指揮の影響を混乱させる古典的な仕組みによるだけではなく、巧みに歪んだ（偽の）情報で誤った方向に導かせることによって実行でき、共通情報通信環境を通じて特定の統治機関に適切に中継できる*[107]。

以前のどのような紛争以上のドンバスにおけるロシアの軍事行動は、実験のための貴重な機会を与えただけではなく、電子戦の土台にある理論と戦闘行動を支援するためのその応用の間のギャップを埋めるものでもあった。これらの機能の多くは、心理戦を支援するための欺瞞情報から、敵の通信とレーダーを妨害し、阻止しまた混乱させ、さらに作戦中に指揮統制を実行する敵の能力を混乱させることにまで及んでいる[108]。

電子戦能力は軍種の武器の地位を達成するのに遠い道のりかもしれないが、確かにロシアの軍事作戦において重要な戦闘支援を提供していることは確かである。ウクライナ軍は、敵対的な電子戦環境で作戦することを学び、また紛争が進展するにつれて進歩を遂げたけれども、ロシアのクリミアおよび南東ウクライナへの介入を支援する電子戦の使用に対して特に準備できていなかった。それにもかかわらず、ロシア軍とその発展する電子戦能力に関する誇張を避けるために、これらの出来事は技術的に劣った敵に直面するという状況で起こったと述べるべきである[109]。そこで、よりよい電子戦能力を開発する上でのロシアの進歩が、NATOと東部地域のその加盟国の安全保障に関して意味することについての問題が生じている。

107）Korolyov, Kozlitin and Nikitin, “Problemy opredeleniya sposobov boevogo primeneniya”, op. cit.
108）Author interviews with Ukrainian EW specialists, Washington DC, June 2017.
109）Author interviews with NATO EW specialists, Washington DC, June 2017.

4．結論－NATO に関しての意味合い

ロシアは、ネットワーク中心能力を備えた実験を含み、情報環境における敵に対する優位性を利用しまた獲得する方法を探求する、戦争に対する革新的なアプローチを採用しようとする取り組みにおいてかなり進歩している。これは主に自動化された C4ISR の統合による意思決定の速さ、また電子戦部隊の役割におけるプロセスを洗練させることに関連している。ロシアの軍事計画者は、軍事学と軍事能力の実際の変化との間のギャップを狭めてきた[110]。電子戦は、ロシアの最近の戦闘経験で証明されているように、「戦力倍増器」を追求する上でますます重要な役割を果たしている[111]。しかし、ウクライナ南東部の作戦を支援するための電子戦アセットの活用は、NATO 側がキエフ(ウクライナ)の負うことのできない高度な技術的アセットを展開できるため、それだけでは NATO の教訓は非常に限定されている。さらに、電磁波スペクトラムを完全に技術的に劣化させることができるとのロシアの主張は、明らかに誤っている。

それにもかかわらず、ロシア軍による電子戦の進歩と、軍事近代化と変革におけるこれらの傾向の長期的一貫性については、NATO 側にとって重要な意味がある。とりわけ、ロシア軍の進行中の変革の最終結果は、このような「戦力倍増器」によって、1990年代のソビエト連邦軍によって保有されていた能力を超えた通常戦能力を提供するという認識を必要とする[112]。ロシアとの紛争が NATO の東部地域で勃発する場合、活動の最初の兆候は電磁波スペクトラムにあり、この領域で主導権と優位性が決定されるであろう。モスクワは、これを NATO 側の弱点の可能性がある領域と認識しているようにみえるため、この能力をさらに強化するために投資した。これは、NATO が政策、教義、組織、能力、訓練、戦術と手順、および演習シナリオに対する方法を変えなければならないことを意味している[113]。

これらの進歩は、一部の米国電子戦将校によって認識されることになった。2015年12月に、国防総省の電子戦部の陸軍主任幕僚ジェフリー・チャーチ（Jeffrey Church）大佐は、ロシア軍が電子戦の面で米国の組織を組織的に上回っている可能性があることを明らかにした。ワシントン DC の電子戦専門家の会合に向けて、チャーチは次のとおり説明した。

ロシア人は電子戦に対して訓練している。彼らは電子戦部隊を持っており、訓練された兵士が使

110) Lastochkin and Falichev, “Kupol nad Minoborony”, op. cit.; Korolyov Kozlitin and Nikitin, “Problemy opredeleniya sposobov boevogo primeneniya”, op. cit.
111) Gusarov, “Taktika rossiyskikh grupp REB”, op. cit.
112) Ivanov, “Soderzhanie i rol’radioelektronoy bor’by”, op. cit.
113) Lastochkin and Falichev, “Oruzhiye asimmetrichnogo otveta”, op. cit.; Valagin, “Strategicheskaya sistema REB”, op. cit.; Tikhanychev, “O roli sistematicheskogo ognevogo vozdei’stviya”, op. cit.

用する電子戦装備を持っており、またそれを訓練に組み込んでいる。我々は電子戦部隊を持っておらず、装備はほとんどなく、電子戦訓練はほとんど行っていない。我々は彼らと同等またはそれ以上のものではないというわけではない。我々がそうしないことを選択したからである[114]。

また、そのような議論は、2017年初頭に新しい米国電子戦戦略を策定し実行するための取り組みに確かに貢献した。また、NATO側は、電磁波スペクトラムにおける競争相手としてのロシアの出現に関する無知を是正するために多くの行うべきことがある。しかし、バルト地域の安心と抑止の取り組みを強化するという観点から、NATOは、前述の相当なロシアの電子戦能力を念頭に置いて、進んでいくには長い道のりがある。なぜならば、この電子戦能力はロシアのA2／AD方法に入っているからである。

バルト諸国の安全保障を強化する上で、同盟側にとって潜在的に重要なパートナーはイスラエルである。電子戦に関する協力はイスラエルと米国の間に長く存在しており、これはNATO側の他の加盟国にも拡大され得る。バルト諸国はすでに「技術に精通している」ため、効果的な電子戦とサイバー戦能力を強化するための既存の基盤が存在する。すなわち、イスラエルの専門家は、潜在的な電波管制に対応し、ロシアの傍受の有効性を制限するのに役立つために、バルト地域のSIGINT能力の開発を支援できる。また、イスラエルの電子戦専門家も、実際の戦闘条件でのイスラエル国防軍の広範な経験に基づいて、相互の調整またサイバー攻撃と運動エネルギー攻撃を含むさまざまな電子戦要素の有効性と調整を最大限に引き出す構想を策定するための貴重な支援を提供できる[115]。

同様に、イスラエルの電子戦専門家は、NATO側のUAV搭載電子戦能力の開発を支援できる。なぜならば、より高機能かつ高価なUASが展開され、特に高烈度電磁波スペクトラム環境で作戦すると予想されるため、UASの電子防護（EP）機能と電子攻撃（EA）能力が重要になっている。イスラエルは、NATO能力に追加できるUASのEPとEAの両方のソリューションを提供している[116]。イスラエルとの潜在的協力の一例は、IAI Harpy（パッシブレーダー・シーカーを使用する）のような安価な徘徊型兵器（loitering munition）の分野にある。この兵器はNATOの欧州加盟国に限られた敵防空網制圧（SEAD）能力を付与されたNATO側によって優先させるべきである。ロシアの雑音妨害器に対する非常に効果的で比較的低コストの解決策を潜在的に証明する可能性があるので、妨害に向かって進む（home-on-jam）徘徊型兵器の共同開発が考慮されるべきである[117]。

114) Ellen Mitchell, “Army’s electronic-warfare training seen as lagging behind Russian efforts”, Inside Defense, December 8, 2015, https://insidedefense.com/inside-army/armys-electronic-warfare-training-seen-lagging-behind-russian-efforts (accessed July 10, 2017).
115) Author interviews with NATO EW specialists, Brussels, June 2017.
116) Author interviews with Israeli defence specialists, Washington DC, June 2017.
117) These munitions are designed to detect and destroy GPS jammers.

しかし、NATOは、最初にバルト諸国の電子戦能力を強化し、発展するロシアのA2／AD能力に対する防御を強化するとともに、C4ISRを攻勢的な強力なツールの範囲で近代化し統合するモスクワの取り組みを考慮することに目を向けなければならない。A2／AD方法に深みと信頼性を加えたロシアの電子戦の進歩は、次にNATOに対するアクセスを得るための新しい手段を見つけるために、運動エネルギー問題（目標に対する爆弾）というよりも運動エネルギー／非運動エネルギー統合問題（宇宙、サイバー、および電磁波スペクトラムを活用する）として枠組みされた問題に取り組ませるであろう。また、これには、作戦レベルの司令官とその計画立案者に戦場に出現する時に機会を利用できるタイムライン内の多様な能力を一体化する権限（実際に戦術的統制）を可能にする指揮統制系統の創設を含んでいる[118]。たとえば、空中領域では、NATOは状況認識を提供し、戦術アセットを作戦上の意思決定者にリアルタイムで直結させる堅牢な戦術ネットワークを享受してきた。困難な電磁波スペクトラム環境における作戦は、独特で困難である。NATO軍は、航空優勢が作戦を可能にするための特定の位置の特定の時刻に接続性のポケットを作り出すと考えられる方法で戦術的な接続性を調べる必要があるかもしれない[119]。

モスクワは、限られた手段や国内国防産業のより広範な復興を阻む多くの課題であっても、技術面での追いつき政策に着手したが、NATOがロシアの通常戦攻撃能力を再構築するプログラムに対処しない限り、その格差は主要分野で縮小している。さらに、それと同等に重要なのは、電子戦開発を補完するために、その教義的方法にもっと柔軟な立場を導入したことである。NATOに類似した戦闘に対するロシアの方法のパラダイムシフトと、ネットワーク化された指揮統制およびこれらの非常に有能な脅威システムの統合による重要な推進役としての電子戦の採用は、高度な情報戦と結合して、どのような将来の紛争においても、NATOとロシアの間の競争の場面を非常に迅速に平衡状態にするであろう。ロシアの電子戦能力は、電子戦の観点だけではなく、高烈度の電磁波スペクトラム戦闘空間における電磁機動としてもみられるべきである。結果として、ロシアの通常戦軍事能力の開発における他の要因よりも、この分析が正しい場合、電子戦はNATOにとって基本的かつ長期的な課題を提起する。

118）Author interviews with NATO EW specialists, Brussels, June 2017.
119）Author interviews with NATO EW specialists, Brussels, June 2017.

附属書 A

電磁波放射スペクトラムおよび軍民用途[120)]

周波数帯		波長帯		用途	
周波数帯 名称	周波数	波長帯	波長名	民間	軍用
	Up to 300 mHz	1 Mmまで	極超長波		地震音響兵器
HLF	300-3000 mHz	1-10 Mm		地球物理学研究	
ELF	3-30 Hz	10-100Mm			
SLF	30-300 Hz	1000-10,000 km			潜水艦通信
ULF	300-3000 Hz	100-1000 km			
VLF	3-30 KHz	10-100 m	超長波	水中音響局	
LF	3-300 KHz	1-10 km	長波	無線航法システム	
MF	300-3000 KHz	100-1000 m	中波	ラジオ放送，海上移動体通信	
HF	3-30 MHz	10-100m	短波	無線放送，海上移動体通信，医用超音波スキャナー	戦術レベル無線通信，超水平線レーダー
VHF	30-300 MHz	1-10 m	超短波	ラジオ，テレビ放送	戦術レベル無線通信，長距離レーダー探知
UHF	300-3000 MHz	1-10 dm	極超短波	衛星航法システム,衛星通信システム	
				ネットワーク通信，海上移動体通信，テレビ放送	ミサイル攻撃早期警戒システム，移動体無線周波数
SHF	3-30 GHz	1-10 cm	センチメートル波	衛星通信システム，無線中継通信，対流圏通信，無線コンピューターネットワーク	
				民間レーダー（航法および航空管制用）	軍用レーダー（地上、海上および航空目標探知、火器管制）
EHF	30-300 GHz	1-10 mm	ミリ波	電波天文学，高速無線中継通信，民間レーダー（気象）	移動体無線武器システム，軍用レーダー（弾道ミサイル・宇宙物体追跡、地上移動目標偵察），自動データ伝送システム，広帯域通信システム
HHF	300-3000 GHz	0,1-1 m	サブミリ波	検査スキャナー,医用断層撮影	高高度および宇宙用高速通信・位置決めシステム

120) Shepovalenko, “Boevye lazery budushchikh voyn”.

附属書 B

ロシアの電子戦システム

電子戦システム	目　　的
RB-301B	HF／VHF／UHF 通信の妨害すること。 RK-330KMV 指揮所 R-378BMV、R-330BMV、R-934BMV and R-325UMV 妨害ステーション http://www.sozvezdie.su/newspaper/_22_dekabr_2009_g/borisoglebsk2noviy_kompleks/ http://www.efirzavod.ru/index.php?id=37
1L269 Krasukha-2-O	S バンドレーダー（典型的に早期警戒管制機に使用されている）を妨害すること。 http://kret.com/products/radioelektronnaya-borba/kompleks-radioelektronnoy-borby-krasukha-2-o/
1RL257 Krasukha-C4	X／Ku バンド火器管制レーダー（典型的には戦闘機に使用されている）を妨害すること。 http://kret.com/products/radioelektronnaya-borba/kompleks-radioelektronnoy-borby-krasukha-s4/
Moskva- 1	ESM システム 1L265　パッシブ探知局。航空機レーダー放射の方向探知の検知、識別。 1L266　航空機レーダー妨害用妨害局の制御コマンドポスト http://kret.com/products/radioelektronnaya-borba/stantsiya-radioelektronnoy-razvedki-moskva-1e/
SPR-2M Rtut-BM	通信、無線近接信管および遠隔起爆信号を妨害すること。 http://kret.com/products/radioelektronnaya-borba/kompleks-radioelektronnoy-borby-rtut-bm/
RB-531B Infauna	通信、無線近接信管および遠隔起爆信号を妨害すること。また、ミサイル発射および煙の自動放出の光学検知。 https://rg.ru/2014/04/30/reb-site.html
Lesochek	通信、無線近接信管および遠隔起爆信号を妨害すること。コンパクト－携帯可能。 https://rg.ru/2014/04/30/reb-site.html
Pole-21	GPS 信号を妨害すること。 R-340RP jamming stations that are mounted on cell mobile phone towers. http://iz.ru/news/628766#ixzz4IHrzF0Xl
RP-377LA Lorandit	HF／VHF／UHF 通信の探知、方向探知および電波妨害を行うこと。 https://reb.informost.ru/2014/pdf/1-8.pdf http://forums.airbase.ru/2014/05/t89725--sredstva-reb-i-rtr-podrazdelenij-vdv.html

Magniy-REB	電子戦専門家の訓練用。 http://syria.mil.ru/news/more.htm?id=12054820@egNews
Leer- 2	通信を妨害すること。 http://www.armyrecognition.com/russia_russian_army_wheeled_armoured_vehicle_uk/tigr-m_mktk_rei_pp_leer-2_vpk-233114_mobile_electronic_warfare_ew_vehicle_technical_data_sheet.html
RB-341V Leer- 3	携帯電話（GSM）網を妨害すること。 指揮統制および妨害器装備の 3 機の Orlan-10 UAV を含む。また、携帯電話に SMS メッセージを送信できる。 Leer-3s は 3 G および 4 G で作動するように明らかに性能向上された。しかし、これは未検証である。 http://iz.ru/news/659503
Less	自動指揮統制。データの収集・処理を行い、電子防護／電波管制システムを統制すること。 https://reb.informost.ru/2014/pdf/1-8.pdf
RB-636M2 Svet-KU	電子防護／電波管制システム。電磁波状況評価用。放射源の探知、分析および方向探知を行う。 https://reb.informost.ru/2014/pdf/1-8.pdf http://bastion-karpenko.ru/svet-ku/
Alurgit	当該システムに関する信頼できる情報はない。
Parodist	当該システムに関する信頼できる情報はない。