

警察政策学会資料 第 125 号  
令和 4 (2022) 年 9 月 初版  
令和 4 (2022) 年 12 月改訂版  
令和 5 (2023) 年 7 月再訂版

# ウクライナ戦争の教訓

## ～我が国インテリジェンス強化の方向性～

警察政策学会テロ・安保問題研究部会

茂 田 忠 良

## 「再訂版の発行について」

本論考の初版は、2022年9月に『ウクライナ戦争の教訓～我が国インテリジェンス強化の方向性～』と題して発行した。ロシア・ウクライナ戦争においてインテリジェンスが果たしている役割、そこから導き出せる我が国への教訓について、2022年8月までの状況を前提として記述したものである。

その後、戦況の推移につれてインテリジェンス関連でも新しい展開があったこと、また新たに入手できた資料があったことなどのため、大幅に加筆して、同年12月に改訂版を発行した。

更に2023年4月には、マサチューセッツ州の空軍州兵ジャック・テシェイラによる情報漏洩が発覚し、漏洩情報によって米国インテリジェンスの情報収集力の実態がより明らかになった。また、その他にも新たな資料の報道や公開があった。そこで、今回2023年7月まで得られた情報の中でも重要と考えられるものを加筆して、再訂版を発行した。今回の加筆部分は青色で示している。また、この機会に言い回しの修正など字句の補正も行った。

なお、テシェイラによる情報漏洩に関しては、別途分析して『Teixeira 漏洩情報に見る米国インテリジェンス力』（警察政策学会資料第129号、2023年）として発行するので、そちらを参照されたい。

令和5年（2023）7月

テロ・安保問題研究部会長

茂田忠良

# ウクライナ戦争の教訓～我が国インテリジェンス強化の方向性 (再訂版)

元内閣衛星情報センター次長

元防衛庁情報本部電波部長

茂田インテリジェンス研究室 茂田忠良

## <目次>

初めに (本稿の目的)	1
1 戦況の推移	2
(1) 第1期：全面侵攻とキエフ攻防戦 (2022年2月24日～3月)	
(2) 第2期：ロシア軍の東部占領攻防 (4月～8月)	
(3) 第3期：ウクライナ軍反攻 (8月末～11月)	
(4) 第4期：バフムート攻防戦と戦線膠着 (12月～2023年5月)	
(5) 第5期：ウクライナ軍の反攻と戦線膠着 (6月～7月)	
(6) サイバー攻撃・情報作戦	
2 ウクライナ善戦の背景	7
(1) ロシア側の要因	
(2) ウクライナ側の要因	
3 米国政府の対応に見るインテリジェンス力の現れ	13
(1) ロシアのウクライナ全面侵攻の予測と対応準備	
(2) 米国による情報作戦	
(3) 侵攻開始直前の米国政府の行動	
(4) 米国のウクライナに対する情報支援の恒常化	
(5) プーチンによる核ブラフへの対応	
(6) 米国インテリジェンスの限界	
4 米インテリジェンス諸機関の情報収集力の骨格	19
(1) シギント・プラットフォーム	
(2) イミント・プラットフォーム	
(3) マシント・プラットフォーム	

5	米国によるインテリジェンス支援	25
	(1) 情報提供方針・提供情報内容	
	(2) インテリジェンス支援の方法	
	(3) インテリジェンス支援の成果	
	(4) サイバー防衛支援	
	(5) 補足：ウクライナ支援と Give & Take の原則	
6	ウクライナ SSU によるインテリジェンス	40
	(1) ウクライナ・セキュリティ・サービス SSU	
	(2) 広汎な通信傍受能力と作戦支援	
	(3) 国民からの情報収集の組織化	
	(4) ロシア工作員・協力者の摘発	
	(5) サイバー攻撃対策	
	(6) 情報作戦	
	(7) 徴兵逃れの阻止・摘発	
	(8) まとめ	
7	教訓：我が国インテリジェンス強化の方向性	59
	(1) 国家シグント機関の創設	
	(2) 国家イミント機関の創設	
	(3) セキュリティ・サービスの創設	

## 初めに（本稿の目的）

2022年2月24日にロシア軍がウクライナに全面侵攻を始めて以来、ロシア・ウクライナ戦争が続いている。開戦前の大方の予想に反して、ウクライナが善戦している。その要因は幾つが挙げられるが、要因の一つが、ウクライナ側のインテリジェンス優位である。

このインテリジェンスの重要性に着目して、宮家邦彦氏など一部の有識者は、日本も本格的な対外諜報機関を創設すべし、と提唱している<sup>1</sup>。確かに我が国にとってインテリジェンス強化は焦眉の急である。しかし、具体的にどうすればインテリジェンスを強化できるのか。本格的対外諜報機関の創設と言っても、それはそもそもどのような機関なのか。ヒューメント機関なのか。或いはそれ以外の機関なのか。また、我が国独力で実力ある諜報機関の創設が可能なのか。つまり、具体的にどうすれば、必要なインテリジェンスを得る態勢をとることができるのかについての論究は見当たらない。

因みに、フランスやドイツの諜報機関は、ロシア軍の全面侵攻を予測できなかった。そのため2022年3月にはフランス軍情報局長官が辞任している<sup>2</sup>。フランスやドイツは、我が国と比較して遥かに優れたインテリジェンス諸機関を有しているが、その両国にしてこうなのである。

それではウクライナのインテリジェンス優位の実態は如何なるものであろうか。それは第1に、米国のインテリジェンス支援である。米国は、世界最高のインテリジェンス力を使って、ウクライナの戦争努力を全面的に支援している。某米国政府職員は、米国は非NATO加盟国に対する情報協力としては未曾有の大量の情報支援をしており、それが質量共により強大なロシア軍との戦いで決定的な役割を果たしていると述べている<sup>3</sup>。次に第2に、ウクライナ自身のインテリジェンス力であり、中でも優秀なセキュリティ・サービスによる貢献である。

我が国にとって適切なインテリジェンスの強化策を考えるには、このような、ウクライナ戦争におけるインテリジェンス優位の実相を知る必要がある。そうすれば、自ずと我が国のインテリジェンス強化の方向性も見えてくるであろう。

そこで本稿では、ロシア・ウクライナ戦争との関連において、先ず基礎知識として、全面侵攻以来の戦況を概観してウクライナ善戦の背景を見た上で、米国のインテリジェンス支援とウクライナのインテリジェンス力について、次の諸点を論ずる。その上で、そこから導かれる我が国におけるインテリジェンス強化への教訓を提示したい。

- 今次戦争における米国政府の対応に見るインテリジェンス力
- 米インテリジェンス諸機関の情報収集力の骨格

---

<sup>1</sup> 宮家邦彦「米国の圧勝か 対露情報戦」『産経新聞』2022年5月5日。

<sup>2</sup> “French intelligence chief Vidaud fired over Russian war failings,” *BBC News*, 31 March 2022, accessed 13 May 2022, <https://www.bbc.com/news/world-europe-60938538>

<sup>3</sup> Ken Dilanian, et.al., “U.S. intel helped Ukraine protect air defenses, shoot down Russian plane carrying hundreds of troops,” *NBC News*, 27 April 2022, accessed 6 May 2022, <https://www.nbcnews.com/politics/national-security/us-intel-helped-ukraine-protect-air-defenses-shoot-russian-plane-carry-rcna26015>.

- 米国によるインテリジェンス支援
- ウクライナのセキュリティ・サービス SSU の活動
- 教訓：我が国におけるインテリジェンス強化の方向性

なお、今回米国は、ロシアによる情報工作に対抗するために、相当量のインテリジェンスを開示している。しかし、それでも、基本的に情報データの収集源・収集方法は機密事項であり、情報開示も一部に過ぎない。従って、米国についての論考は、小生の従来の研究を基礎に、公開情報と報道情報から合理的に解釈したものであり、一部に推論が含まれることをお断りしておく。また、ウクライナのセキュリティ・サービスの活動については同セキュリティ・サービスの公式ウェブサイトによくを負っている。

## 1 戦況の推移<sup>4</sup>

まず、基本知識として、全面侵攻以来の 2022 年 11 月までのロシア・ウクライナ戦争の状況を概観しておきたい。戦況は、概ね、第 1 期：全面侵攻から首都キーウ攻防でロシア軍が首都占領を諦めて撤収するまで、第 2 期：ロシア軍が占領地拡大のために東部で攻勢をかけている時期、第 3 期：ウクライナ軍が東北部ハルキウ州や南部ヘルソン州で反攻勢をかけている時期、そしてその後の膠着状態の時期に分けられる。また、物理的な戦闘の他に、サイバー戦や情報戦も継続して行われている。これらについて、概観したい。

### (1) 第 1 期：全面侵攻とキーウ攻防戦（2022 年 2 月 24 日～3 月）

2022 年 2 月 24 日未明、ロシア軍は、ウクライナの「非軍事化」「非ナチ化」を目的に掲げ、全面侵攻を開始した。先ずロシア空軍が、ウクライナ各地の防空施設、空軍飛行場、兵站拠点など対してミサイルや爆撃機を使って攻撃を行った。同時にロシア陸軍が、ウクライナの北、東北、東、南の 4 方面から侵攻を開始した。4 方面とは、北方の隣国ベラルーシから首都キーウを目指した侵攻、東北からハルキウ州への侵攻、東部ドンバス地方（ルハンシク州とドネツク州）への侵攻、南部クリミアからヘルソン州やザポリージャ州への侵攻である。

ロシア軍は、この全面侵攻によって、数日にしてウクライナを屈服させられると想定していたようである。しかし、予想外のウクライナ軍の抗戦のため、上手くいかず、3 月末には首都キーウ攻略を諦めて、首都攻略部隊は撤退することとなる。

#### ア 首都キーウへの侵攻と占領失敗

ロシア軍の攻撃で最も注目されたのが、首都キーウに対する攻撃である。ロシア軍の作戦計画では、開戦冒頭、首都北西 20 キロにあるホストメリ軍用空港を精鋭の空挺部隊がヘリコプターや輸送機を使用して迅速に占拠する。そして、そこを拠点に電撃的に首都を制圧

---

<sup>4</sup> 本節の資料の多くは、Institute for the Study of War, *UKRAINE CONFLICT UPDATES* に拠っている。<https://www.understandingwar.org/background/ukraine-conflict-updates>

して、ゼレンスキー大統領を排除して傀儡政権を樹立するというものであった。しかし、ウクライナ軍による激しい抵抗のためロシア空挺部隊は大損害を被り、結局ホストメリ軍用空港は占領したものの、電撃的首都制圧には失敗する。

同時にロシア陸軍部隊が、地上をベラルーシから首都キーウに向かって進軍し、ドニプロ河の両岸を南下した。西岸を南下したロシア軍は首都郊外にまで迫りブッチャやイルピンなどで激しい戦闘が行われた。東岸を南下したロシア軍は、国境を超えたチェルニヒフ市で激しい抵抗を受け思うように進撃できなくなった。

また少し遅れてロシア領内から機甲部隊がウクライナ東部のスーミ市を經由して国道7号線を西進して首都に向かったが、2022年3月9日に首都東方のプロバルイでウクライナ軍の待伏せ攻撃を受け大損害を被り、進撃は停止した。

首都攻防戦では、ウクライナ正規軍のみならず、国土防衛隊（義勇兵）、国家警備隊（内務省治安部隊）などの準軍事組織、更には一般国民が自主的に武器を取って参加して、首都キーウを守り通したのである。

ロシア軍は、3月下旬には首都キーウ占領を諦めて、首都攻略部隊を撤収させた。

#### イ ハルキウ州への侵攻

ハルキウ州の侵攻では、ハルキウ市の占領は成し得なかったが、概ね州の東半分はロシア軍が占領した。

#### ウ 東部ドンバス地方（ルハンシク州とドネツク州）への侵攻

ロシア軍は、進撃速度は速くないものの徐々に占領地域を拡大した。3月末にはルハンシク州の大部分を占領し、ドネツク州でも占領地域を拡大した。

#### エ クリミアからヘルソン州・ザポリージャ州への侵攻

ロシア陸軍の4方面からの侵攻では、最も成功した侵攻であり、侵攻翌日にはヘルソン州の州都ヘルソン市に到達し、ヘルソン州とザポリージャ州の大部分を占領した。

#### カ 航空優勢の確保に失敗

現代の戦争では、開戦当初に、戦域、つまり戦闘が行われる地域での航空優勢を確保するのが常道となっている。航空優勢を確保することによって敵軍に対する情報収集や対地攻撃機や戦闘ヘリによる支援によって地上戦闘を有利に進めることができるからである。

ロシア軍も開戦冒頭で、ウクライナの空軍機・空軍飛行場や防空システム（防空レーダ、対空ミサイル、対空機関砲など）を、ミサイルや爆撃機で攻撃したが、十分な成果をあげることができなかった。その原因は、ウクライナ軍が避難などの対抗措置を取ったことと、ロシア軍がウクライナ軍の戦闘意思や能力を過小評価していたためであろう。

緒戦においてウクライナ上空での航空優勢の確保に失敗したことが、その後のロシア軍の苦戦にも繋がってくる<sup>5</sup>。

---

<sup>5</sup> Daniel Michaels, "Failure to Control Ukraine's Skies Betrays Key Flaw in Russia's War Strategy," *The Wall Street Journal*, 17 October 2022, accessed 18 October 2022, [https://www.wsj.com/articles/failure-to-control-ukraines-skies-betrays-key-flaw-in-russias-war-strategy-11665915386?mod=panda\\_wsj\\_custom\\_topic\\_alert](https://www.wsj.com/articles/failure-to-control-ukraines-skies-betrays-key-flaw-in-russias-war-strategy-11665915386?mod=panda_wsj_custom_topic_alert)

## (2) 第2期：ロシア軍の東部占領攻防（2022年4月～8月）

ロシアは2022年3月末には首都キーウ占領とウクライナ政府の転覆を諦めて、当面の目標を東部のドンバス地方の完全占領に変更した。このためロシア軍は首都キーウ周辺から撤収して、東部ドンバス地方の攻撃に力点を移した。4月以降のドンバス地方をめぐる攻防では、ロシア軍が押し気味であり徐々に占領地を拡大していた。しかし、精密攻撃が可能なHIMARS（高機動ロケットシステム）や155ミリ榴弾砲が米国からウクライナ軍に提供され7月に戦場で使われるようになると、後方のロシア軍の指揮所や兵站基地が攻撃を受けるようになってロシア軍の攻撃は停滞し、8月には戦線は膠着状態となった。

この期間の攻防で注目を集めた幾つかの戦闘がある。まず、5月上旬のロシア軍のドネツ川渡河作戦の失敗である。ロシア軍部隊は、ルハンシク州全域を占領するためにドネツ川の渡河作戦を試みたが、渡河作戦中の部隊がウクライナ軍の砲撃を受け大損害を被り渡河作戦は失敗した。

次に、セヴェロドネツク・リシチャンシク攻防戦も注目を集めた。両市はルハンシク州内でウクライナが支配する最後の拠点都市であり、この支配を巡って5月から7月上旬にまで激しい攻防戦が行われて、7月上旬にロシア軍が占領した。

更に、ドネツク州南部の港湾都市マウリポールの戦闘も注目を集めた。同市のウクライナ軍は3月中旬以降完全に包囲され、最後にアゾフスタル製鉄所に籠城して激しく抵抗したが、残存した部隊も5月15日に降伏した。

この期間中は、東部においてロシア軍による若干の占領地の拡大が見られたが、8月に入ると、ロシア軍の低い士気、兵站の悪さ、不適切な指揮命令、そしてウクライナ軍のHIMARSなどによる精密攻撃のため、ロシア軍の戦闘能力は相当低下していった。

## (3) 第3期：ウクライナ軍反攻（2022年8月末～11月）

2022年8月末以降は、ウクライナ軍が反転攻勢に出た時期である。

### ア ハルキウ州奪還（9月7日から）

ウクライナ軍は、9月7日突然ハルキウ州全域の奪還のための攻勢作戦を開始し、ロシア軍の防衛線を突破して7日、8日の2日間で50キロも突出した。虚を突かれたロシア軍は混乱して壊走し、多くの武器弾薬を放置して後退した。

元々ハルキウ州にいたロシア軍精鋭部隊は、ヘルソン州の占領地防衛やドンバス地方における攻勢強化のために、ヘルソン州やドンバス地方に移動していた。ウクライナ軍は、ハルキウ州のロシア軍兵力が手薄になっていたところに攻撃をかけたのである。

攻勢の結果、ウクライナ軍は、約1週間でオスキル川までのハルキウ州の大部分を奪回し、その後進撃速度は低下したものの、10月中旬にはハウキウ州の殆どを奪還した。

### イ ヘルソン州での攻勢（8月29日から）

ウクライナ軍は、ヘルソン州のドニプロ河西岸地区のヘルソン市奪還を目指して8月29日攻撃を開始した。ウクライナ軍は、ロシア軍の地上通信回線や指揮所、それに弾薬庫などを砲撃すると共に、地上部隊も徐々に前進した。ロシア軍は、ドニプロ河西岸に対する補給に困難を生じており、11月11日には西岸を撤収して、ドニプロ河東岸を新しい防衛線とし



た。

#### (4) 第4期：バフムート攻防戦と戦線膠着（2022年12月～2023年5月）

2022年秋以降、ロシアは、民間軍事会社ワグネルの部隊が中心となってドネツク州のバフムート占領を目指して激しく攻撃していたが、ウクライナ軍も激しく抵抗をした。2023年に入って更に攻撃を激化させ、5月になって漸く市街全域を占領した。しかし、この間ウクライナ軍も激しく抵抗したため、両軍に相当な損害が発生し、特にワグネル兵士の死傷者数は甚大であった。

バフムート以外では、ウクライナの気候が泥濘期で戦闘に適していないこともあり戦線は膠着し、この間、ロシア軍は各戦線で防禦陣地の構築を進めた。他方、ウクライナ軍は、西側から戦車や装甲戦闘車の供与を受けて、反攻用の部隊12個旅団約5万人の部隊の訓練に充てた。

#### (5) 第5期：ウクライナ軍の反攻と戦線膠着（2023年6月～7月）

ウクライナ軍は、被占領地の回復を目指して、6月に南部地域、東部地域で反攻を開始したが、ロシア軍は既に各地に強力な防禦陣地を構築しており、他方、ウクライナ軍では反攻に必要な航空戦力などの装備が十分ではなく、反攻は遅々としたものとなっている。

#### (6) サイバー攻撃・情報作戦

ロシア軍は、いわゆるハイブリッド作戦を遂行している。つまり正規軍や非正規軍による物理的攻撃、サイバー攻撃、偽情報を流布させる情報作戦など多様な攻撃を組み合わせているのである。サイバー攻撃や情報作戦も盛んに行われているが、ウクライナ側の対抗措置もあって、致命的な損害は与えていない。攻撃の一例を見てみよう。

##### ア サイバー攻撃

- 2022年1月13日～14日第一波大規模攻撃：政府機関などのウェブサイトに対するDDOS攻撃、データ消去型（ワイパー型）マルウェアによる攻撃が見られた。データ消去型マルウェアによって、政府系のウェブサイト70が一時的に閲覧不能に陥った。
- 同2月15日～16日第二波大規模攻撃：国防省、軍、外務省、電子政府ポータル、国営銀行のウェブサイト到大規模DDOS攻撃が行われ、数時間に亘ってサービス障害が起こった。
- 同2月23日～24日侵攻時の大規模攻撃：ウェブサイトに対するDDOS攻撃や新種のデータ消去型（ワイパー型）マルウェアによる攻撃が行われた。また、欧州の衛星通信KA-SATの通信モデムが攻撃されて通信容量が20%まで激減し、大規模な通信障害が発生した。この攻撃はロシア軍情報部GRUが行ったものであるが、同衛星通信はウクライナ軍が指揮通信やドローン操縦などの戦術通信にも幅広く使用していたため、ウクライナ軍の通

信に相当の打撃を与えた<sup>6</sup>。2022年10月までのサイバー攻撃の中では最も効果を上げた攻撃である<sup>7</sup>。

○ 全面侵攻後もロシアによるサイバー攻撃は継続しているが、致命的な損害は発生していない。2022年4月8日に計画されていたエネルギー関連施設へのサイバー攻撃や6月28日ウクライナの憲法記念日に計画されていたテレビ放送妨害攻撃などは、事前にウクライナ側が探知して未然に防止している。

## イ 情報作戦

ロシアは、多量の偽情報を流しているが、目的の一つはウクライナ軍の士気阻喪である。

○ 2022年2月24日の全面侵攻直後、ベラルーシのハッカー集団 Ghostwriter は、ウクライナ軍関係者のフェイスブックやインスタグラムなどの SNS アカウントに不正にアクセスして、ウクライナ兵が白旗を持って森から出てくる画像を掲載するなど、ウクライナ軍は弱体でロシア軍に降伏しているという情報を流布していた<sup>8・9・10</sup>。これはロシア政府の意向を受けたベラルーシ政府による工作であると見られている。

○ 3月16日に、ゼレンスキー大統領がウクライナ軍にロシア軍への降伏を呼び掛ける動画が、フェイスブック、ユーチューブ、ツイッターなどに投稿された。これは、ディープフェイクと呼ばれる技術で、AI を使用し既存の映像を加工して好みの偽動画を作り出す技術を使ったものである。

ゼレンスキー大統領は、数分後にはフェイスブックに自身の動画を投稿して、偽動画を否定した。また、フェイスブックやユーチューブは偽動画を削除した<sup>11</sup>。

この偽動画は、画像や音声が不自然であったこと、ウクライナ政府が2週間前からディープフェイク動画の投稿があり得ると警告していたこと、大統領本人の否定メッセージが即座に投稿されたことなどから、効果は見られなかった。しかし、仮に偽動画の完成度が高く侵攻直後に投稿されていれば、相当の影響を与えた可能性は否定できない。

---

<sup>6</sup> Ellen Nakashima, “Russian military behind hack of satellite communication devices in Ukraine at war’s outset, U.S. officials say,” *The Washington Post*, 24 March 2022, accessed 27 October 2022, <https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say>

<sup>7</sup> Greg Rattray, “US-Japan Cyber Cooperation and Lessons Learned from Ukraine,” (「ソリトン エグゼクティブフォーラム 2022」講演。東京、2022年10月25日)

<sup>8</sup> Nathaniel Gleicher, “Updates on Our Security Work in Ukraine,” *Meta*, 27 February 2022, accessed 21 October 2022, <https://about.fb.com/news/2022/02/security-updates-ukraine/>

<sup>9</sup> Meta, *Adversarial Threat Report First Quarter 2022*, 7 April 2022, accessed 21 October 2022, <https://about.fb.com/news/2022/04/metas-adversarial-threat-report-q1-2022/>

<sup>10</sup> Sergu Gatlan, “Ukraine links Belarusian hackers to phishing targeting its military,” *Bleeping computer*, 25 February 2022, accessed 22 October 2022, <https://www.bleepingcomputer.com/news/security/ukraine-links-belarusian-hackers-to-phishing-targeting-its-military/>

<sup>11</sup> Tom Simonit, “A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be,” *WIRED*, 17 March 2022, accessed 21 October 2022, <https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/>

## 2 ウクライナ善戦の背景

ロシア・ウクライナ戦争では、開戦前の方の予想に反して、ウクライナが善戦している。善戦の背景には、次の諸要因が挙げられる。先ず、ロシア側の要因としては、①インテリジェンスの失敗、②軍の低い士気、③軍の貧弱な兵站、④軍の硬直した指揮命令・組織体質である。次に、ウクライナ側の要因としては、①国土防衛に向けた軍と国民の高い士気、そして大統領の勇気、②NATO軍に倣った軍改革、③米欧からの潤沢な武器の供与支援、④インテリジェンス力の高さである。それではそれぞれの要因について簡単に見てみよう。

### (1) ロシア側の要因

#### ① インテリジェンスの失敗

ロシアのインテリジェンスの失敗 *intelligence failure* とは、ウクライナの国民意識と抵抗意思を完全に読み間違っていたことである。ロシア軍はウクライナに全面侵攻すれば、容易に現ウクライナ指導部を排除して、ウクライナを支配下に置けると想定していた。ロシア大統領府に対するFSBの報告では、ウクライナでロシア軍の進駐に対して歓迎する者が30%、無関心な者60%で、抵抗する者は10%に過ぎないと見積もられていたという<sup>12</sup>。そのためロシア軍の兵站は長期戦を想定しておらず、戦争をすることを知らされていない兵士もいた程である。

それでは、なぜ、インテリジェンスの失敗が起きたのか。勿論、米国ですら数日或いは1週間でキーウが陥落すると想定していたようであるから、ロシアの失敗も致し方ない面もある。しかし、やはり、その背景には、プーチン始めロシア指導部のイデオロギー・国際秩序観の影響がある。

日本人は、明治以来、近代国際法という欧米規範を受け入れてきた。近代国際法は基本的には主権国家の対等平等を前提としている。つまり国家というものは、国際法上みな対等で平等に扱われるべきであり、それが当然であると思い込んでいる。更に憲法の掲げる「平和主義」に従い、言うことを聞かなかったからと言って勝手に武力を使って制裁したり領土を奪ったりしてはいけないと考えている。そして世界の国々もこの原則を受け入れていると勝手に思い込んでいる。しかし、現実は違うのである。

ロシア政府は2000年代に（他国領土内の住民の）自決権という言葉の使用を始め、2008年にはグルジアに侵攻して南オセチア地方とアブハジア地方に「独立」を宣言させ、実質的に支配するに至った。その際これら地域に対して「特殊権益圏」（影響圏）という言葉を使っている<sup>13</sup>。

また、プーチン大統領は2021年7月に論文「ロシア人とウクライナ人の歴史的一体性について」を発表した。ここで、プーチンは、ロシア人もベラルーシ人もウクライナ人も別の

<sup>12</sup> 「NHKスペシャル『ウクライナ大統領府 軍事侵攻・緊迫の72時間』NHK、2023年2月26日放送。ウクライナのレズニコフ国防相が語ったウクライナ諜報機関が入手した情報。

<sup>13</sup> 袴田茂樹「『プーチンの帝国主義』の背景」『産経新聞』2022年3月23日。同「侵略を許した世界の対露反応」『産経新聞』2022年10月31日。

民族ではなく同じ民族であり、ウクライナはロシアと特別な協力関係を保持するべきである旨を主張している<sup>14</sup>。

これらの言動に見られるプーチンやロシア指導部の国際秩序観は、ソ連時代の「制限主権論」やロシア帝国時代の勢力圏の思想の融合体に近いものと考えられる。一言で言えば、ロシアの勢力は国境を超えて旧ソ連邦諸国にも及ぶべきであるという国際秩序観である。それは、ウクライナなど旧ソ連邦諸国家（バルト三国を除く）に対する諜報をセキュリティ・サービス機関 FSB 第 5 総局の所管としていることにも顕れている。

そもそもセキュリティ・サービスとは、自国や植民地など、自国の支配領域のセキュリティのために活動するインテリジェンス機関である。ウクライナを対外諜報機関 SVR の所管ではなくセキュリティ・サービスである FSB（連邦保安局）の所管としている事実は、その時点で既にウクライナをロシアと対等の主権国家ではなく勢力圏内の地域であるという制度的表明である。その上、専制指導者プーチンが、ウクライナ人とロシア人は同一民族であるという論文まで発表しているのである。そのロシアの FSB 諜報員が、ウクライナ国民の独立意識は強く、ロシア軍が仮に侵攻した場合には頑強に抵抗するだろうという報告書を提出するには相当の勇気がある。仮に一部にそのような報告があったとしても、FSB 第 5 総局という官僚組織における総合分析の過程で、どれだけ重視されたか疑問である<sup>15</sup>。その結果がロシア軍に抵抗する者は 10%に過ぎないという見積もりになったのであろう。

我々もロシアの失敗の教訓を学ぶ必要がある。即ち、インテリジェンス分析においては、常に自己の持つイデオロギー・国際秩序観を当然視せずに対象化し、相手側・関係諸国の持つイデオロギー・世界観を客観的に分析することである。米国は昨年後半以来、ロシア軍の全面侵攻の危険性を度々指摘してきたが、侵攻直前でも我が国のロシア研究者で全面侵攻を予想した者は少なかった。これは自己の国際秩序観、即ち「平和主義」というイデオロギーを相対化することが出来ていないためである。我が国の近隣にも近代国際法を全面的には受容していない国が存在する。中国は、近代国際法を西洋帝国主義が創った欧米に都合の良い規範であるとして、その「合理化」「民主化」（という改変）を目指しているのを忘れてはならない。

## ② 軍の低い士気

そもそも今回のロシア・ウクライナ戦争は、ロシア指導部がウクライナを支配下に置こうという目的で一方向的に始めたものであり、一般国民にとっては開戦の必要性、自分の命を懸

---

<sup>14</sup> ウラジミール・プーチン「ロシア人とウクライナ人の歴史的一体性について」2021年7月12日。<http://www.a-saida.jp/putin/putin.html>

—松里公孝「ロシアのウクライナ侵攻」NIRA 総合研究開発機構、2022年5月13日。  
<https://www.nira.or.jp/paper/research-report/2022/032205.html>

<sup>15</sup> 今回のウクライナ侵攻では、ショイグ国防相が慎重姿勢であったのに対して、パトルシェフ安全保障会議書記とポルトニコフ FSB 長官が強く進言したと報道されている。FSB 長官が主戦論であった事実は、正に FSB の「インテリジェンスの失敗」を象徴するような事実ではないだろうか。

「元 KGB 側近 2 人がプーチン氏に進言 ウクライナ侵攻『今しかない』英紙」時事通信 2022年11月4日、<https://news.yahoo.co.jp/articles/34a54e7b1207dfc4c090dc8293dd2ff089e5b59c>

ける必要がある戦争であると十分に納得できるものではなかった。一方、侵攻部隊では、事前に実戦であると知らされずに従軍した兵士も多数を占めるなど、侵攻の必要性についての情報提供が十分に行われたとも思われない。

ロシアのプーチン指導部は、ウクライナの「ナチ化」などを宣伝していたが、ロシア国民は自分の命を懸ける必要があるとまでは浸透していなかったと見られる。それがために、全面侵攻が始まると、多くのロシア人が徴兵を逃れるために出国をしている。軍の低い士気の一つの表れであろう<sup>16</sup>。

### ③ 軍の貧弱な兵站

ロシア軍の兵站は貧弱である。これは元々の兵站軽視に加えて、軍内の腐敗が原因である。

先ず、貧弱な兵站は、侵攻部隊の食糧不足や隊員の貧弱な個人装備品という形で作戦に支障を来している。食糧不足では、侵攻部隊が、携行食の不足のため、食糧を求めてウクライナ人の民家に押し入ったり、犬を捕獲して食べたりする事例が知られている。また、防寒機能を備えた軍服が不足しており兵士が寒さに震えたり、個人用の救急キットの不足から負傷しても適切な救急措置が取れない事例が多発している。

作戦に必要な装備品についても、例えば、首都キーウ攻略部隊では、トラックのタイヤの地形不適合や整備不良が続出して、部隊運用に支障が生じたと言われる。

このような貧弱な兵站の背景には、軍内の腐敗、つまり将校や兵士による軍需物資の横流しがある。そのために、防弾チョッキ、軍靴、ディーゼル油、石鹼、トイレトペーパー、靴下に至るまで横流しされ、兵士の装備品が不足するのである<sup>17</sup>。

### ④ 軍の硬直した指揮命令・組織体質

ロシア式の指揮命令とは、将軍などの高級将校が作戦を決定し、現場の下級将校や下士官に裁量を認めない方式である。戦場の状況は、刻々変化するのであり、ロシア式の指揮命令では、戦場の状況変化に柔軟に対応した戦闘が実行できない。また、ロシア軍は、上級将校でもその経験が特定軍種に偏っており、軍種を超えた経験が不足していると言われる。そのため、現代戦で重要なエア・ランド・バトル（空地共同作戦）など多軍種に亘る作戦指揮が下手である。更に作戦将校の兵站に対する知識や経験が十分ではなく、兵站軽視の部隊運用をしてしまい、これが部隊の戦闘力を減殺してしまうという。

## （２）ウクライナ側の要因

### ① 国土防衛に向けた軍と国民の高い士気、そして大統領の勇気

<sup>16</sup> 兵士の低い士気を反映したためか、今次戦争では、ロシア軍は兵士の退却阻止部隊（退却する兵士を銃撃する）を配置しています。SSU, “SSU interrogates FSB serviceman who led ruscist anti-retreat squad (video),” *News*, 12 June 2023, accessed 18 June 2023, <https://ssu.gov.ua/en/novyny/ssu-interrogates-fsb-serviceman-who-led-ruscist-antiretreat-squad-video>

<sup>17</sup> Institute for the Study of War, “Russian Offensive Campaign Assessment, October 10,” *Ukraine Conflict Updates*, 10 October 2022, accessed 13 October 2022, <https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-october-10>

ウクライナ軍や国民の国土防衛に向けた高い士気は注目に値する。それはこの戦争が正にウクライナ国家の存続、ウクライナ民族の存続を賭けた闘いであり、多くの国民がそれを認識しているからであろう。

特に、首都キーウ防衛戦での民間人の活躍<sup>18</sup>は注目される。国土防衛隊（志願兵）や国家警備隊（内務省治安部隊）など準軍事組織に属する隊員は当然として、純然たる民間人までが自主的に武器を持って戦闘に参加している。自分達だけで自発的にバリケードを構築して防衛に付いたり、或いは、正規軍と共同して防衛に従事している。更に、兵士に対する食糧や睡眠場所の提供、情報収集それも単に目撃した情報を当局に提供するだけでなく、中には、占領地域内のパン屋が我が身の危険を顧みずに積極的に情報収集をして報告をした例までもある。他の占領地でも、パルチザンが組織され多くの住民が参加しているなど、国民の高い士気の現れである。

更に、ゼレンスキー大統領個人の勇気は特筆に値する。ゼレンスキー大統領は元々喜劇俳優であり、大統領としての資質には疑問符が付けられていた。特に戦争など危機における指導者としては余り期待されていなかった。ところが、ロシア軍の全面侵攻、そして今にも首都キーウ陥落かという瀬戸際で大統領としての本領を發揮したのである。全面侵攻直後に、大統領側近<sup>19</sup>は大統領に首都脱出を勧めた。しかし、ゼレンスキーは、自分個人の命の心配よりももっと大切なやるべきことがあるだろうと、脱出を拒否したのである。首都に留まり国民を鼓舞する映像をフェイスブックなどSNSで送り続けた。また、米国が首都脱出・亡命政権の樹立を提案したのに対して、ゼレンスキーはこれを拒否して「脱出手段ではなく、武器をくれ」と応じたと報じられている。EU首脳とのテレビ会談でも、これが生きて会える最後かもしれないと述べながら支援を要請した。彼は自分の死を覚悟して、自分の死をもカードとして使って、対ロシア防衛戦争を鼓舞し指導した。私利私欲を捨てて行うべきことを行うという危機対処の要諦を実践したのである。

因みに、武士道で有名な山本常朝『葉隠』の書には次の有名な一節がある。「武士道とは死ぬことと見つけたり。二つ二つの場にて、早く死方（しぬかた）に片付くばかり也。別に子細なし。胸すわって進む也。」即ち、生きるか死ぬかの岐路において、死ぬ覚悟を固める（自分にとっての最悪を覚悟する）ことである。その上で、その最悪の事態も選択肢としながら、肚を据えて自分が進むべき道を邁進するということである。

或いは、新渡戸稲造『武士道』は義勇について林子平の次の言葉を引用している。「義は勇の相手にして裁断の心なり。道理に任せて決定して猶予せざる心をいふなり。死すべき場にて死し、討つべき場にて討つことなり。」つまり、必要であれば、自分の命や他人の命よりも道理を優先することが義勇であると述べている。

ゼレンスキーは『葉隠』や『武士道』が示す危機対処の要諦を見事に実践したのである。

---

<sup>18</sup> James Marson, "The Ragtag Army That Won the Battle of Kyiv and Saved Ukraine," *The Wall Street Journal*, 20 September 2022, 10 October 2022, <https://www.wsj.com/articles/russian-invasion-ukraine-battle-of-kyiv-ragtag-army-11663683336>

<sup>19</sup> 首都脱出を勧めた大統領側近とは、大統領府顧問アレクシー・アレストビッチである。前掲「NHKスペシャル『ウクライナ大統領府 軍事侵攻・緊迫の72時間』」

ゼレンスキーになぜそれが出来たのか。筆者は、彼の俳優経験が役立っているのではないかと考えている。理想の大統領であればどう行動するだろうかと考えながら、彼は理想の大統領を演じているのであろう。危機の指導者は、期待される役柄を演ずることが重要なのである。

## ② NATO 軍に倣った軍改革

ウクライナは 2014 年の「尊厳革命」によって親ロシア政権が崩壊し親欧政権が樹立された。ロシアはこれに反発して、クリミア半島を占領して併合、また、東部ドンバス地方の一部に親ロシア派民兵による支配地域を作り出した。その際、ウクライナの軍やインテリジェンス機関は殆ど抵抗することが出来なかった。

そこで、ウクライナは米国と NATO 諸国に協力を求め、ウクライナ軍とインテリジェンス機関の変革強化を進めてきた。

ウクライナ軍の改革では、先ず米軍は 2015 年に 300 人の教官を派遣して基礎訓練から開始した<sup>20</sup>。その後、毎年 1 万人以上の兵士が NATO 軍との共同訓練に参加し、ロシア式の硬直した指揮命令方式・組織体質を欧米型に改革してきた。欧米型とは、刻々変化する戦場の状況に柔軟に対応して、下級将校や下士官などによる現場の判断と裁量を重視する方式・組織である。また、武器についても、ウクライナ西部ヤヴォリウ訓練場で、欧米の提供する武器の使用訓練も行ってきた。例えば、今回の戦争でも活躍している米軍のジャベリン対戦車ミサイルや英軍の NLAW 対戦車ミサイルの取扱訓練である。2021 年にロシア軍侵攻の脅威が増すに従って、訓練も加速していった。そして、2022 年 2 月には既にロシア軍の全面侵攻に対する作戦計画も立案されていたのである<sup>21</sup>。

またウクライナは、特殊部隊の戦闘法も修得していた。即ち、2014 年以降 CIA は、ウクライナ東部ドンバス地方に特殊部隊員を派遣して、同地のウクライナ特殊部隊<sup>22</sup>の気概を確認した上で、各種の特殊戦闘法を訓練している。即ち、ウクライナ側は当初、塹壕で携帯電話を使用しており、ロシア側は、ドローンや通信受信設備などを使用してウクライナ部隊の携帯電話ほか電子機器の位置を測定し砲撃攻撃をしていた。そこで、位置特定の回避技術、戦場での探知回避技術、秘匿通信手段を開発教育すると共に、狙撃技術訓練、ジャベリン対戦車ミサイル等の武器取扱訓練も行った<sup>23</sup>。2015 年には、CIA は米国本土内でも、特殊作

---

<sup>20</sup> Andrew Kramer, “Battle Tested, Ukraine Troops Now Get U.S. Basic Training,” *The New York Times*, 9 May 2015, accessed 12 June 2022, <https://www.nytimes.com/2015/05/10/world/europe/ukraine-troops-receive-us-basic-training-after-battle.html>

<sup>21</sup> Daniel Michaels, “The Secret of Ukraine’s Military Success: Years of NATO Training,” *The Wall Street Journal*, 13 April 2022, accessed 26 May 2022, <https://www.wsj.com/articles/ukraine-military-success-years-of-nato-training-11649861339>. 少なくとも、ウクライナ軍統合作戦司令部では、ロシア軍の多方向からの全面侵攻の可能性も考慮して防衛計画を立案していた。

<sup>22</sup> ウクライナ特殊部隊の所属は示されていないが、状況から判断して、セキュリティ・サービス SSU の特殊部隊アルファと推定する。

<sup>23</sup> Zach Dorfman, “Exclusive: Secret CIA training program in Ukraine helped Kyiv prepare for Russian invasion,” *Yahoo News*, 16 March 2022, accessed 14 April 2022, <https://news.yahoo.com/exclusive-secret-cia-training-program-in-ukraine-helped-kyiv-prepare-for>

戦部隊、諜報部隊の訓練を開始し、火器取扱、偽装技術、秘匿通信などを教育してきた<sup>24</sup>。

更に、ウクライナは、弱者の戦法として、米軍の支援を受けて、ロシア軍占領地におけるパルチザンの訓練と準備もしてきた。パルチザンとは、占領地住民による抵抗運動であり、正規軍による攻撃標的などの情報提供、鉄道など兵站施設に対する破壊活動、ロシア占領当局に対する積極的協力者の暗殺などを行うものである。そのために必要な爆薬、小銃など必要物資を、既に2015年頃から占領予測地に隠匿保管を始めていた<sup>25</sup>。この戦法は、米軍がアフガニスタンやイラクにおける経験から「抵抗作戦構想」(ROC: Resistance Operating Concept)として体系化したものであるが、そのノウハウをウクライナに提供してきたのである。

### ③ 米欧からの潤沢な武器の供与支援

ウクライナ軍に対しては、米国を初め NATO 諸国が膨大な武器の支援をしている。これらの支援がなければ、ウクライナは武器・装備・人員全ての点で上回るロシア軍に対抗できなかったであろう。

NATO 諸国の中でも米国は、多額且つ有用な武器の支援をしており、開戦当初は全体の支援額の3分の2程を支援していた。その後、他の西欧諸国の支援額も増加してきたが、2023年に入っても軍事支援の半分は米国である。そこで、米国による武器支援を見てみよう。

国防総省の広報資料<sup>26</sup>に拠れば、米国政府は、多様な武器の供与や武器使用訓練、維持管理などで、2022年2月24日の全面侵攻以来11月10日までの間に合計186億ドル以上(2021年初以来では合計193億ドル以上)の武器支援を約束している。更に、その支援の多くは、国防総省の武器庫からの現物供与であり、即座に使用できるものである。11月10日に表明された追加支援は、2021年8月以来25回目の武器庫からの現物供与であった<sup>27</sup>。

2022年11月までに供与された(供与の約束を含む)主要な武器システムは次の通りである。

- ・ スティンガー携帯式防空ミサイル 1600 式以上。
- ・ ジャベリン対戦車ミサイル 8500 式以上；その他の対戦車システム 38000 式以上。  
TOW 対戦車ミサイル 1500 式
- ・ スイッチブレイド無人攻撃機 700 機以上；  
フェニックス・ゴースト無人攻撃機 1800 機
- ・ 155mm 榴弾砲 142 門；精密誘導砲弾 4000 発、対戦車地雷弾 9000 発、  
他一般砲弾多数。

[russian-invasion-090052743.html](https://www.defense.gov/News/News-Stories/Article/Article/3216745/400-million-security-package-headed-to-ukraine/)

<sup>24</sup> Ibid.

<sup>25</sup> 「報道1930」BS-TBS、2022年11月10日放送。

<sup>26</sup> DoD, *Fact Sheet on U.S. Security Assistance to Ukraine, November 10, 2022*, accessed 11 November 2022, <https://media.defense.gov/2022/Nov/10/2003113149/-1/-1/1/UKRAINE-FACT-SHEET-NOV-10.PDF>

<sup>27</sup> C. Todd Lopez, “\$400 Million Security Package Headed to Ukraine,” *DOD News*, 10 November 2022, accessed 11 November 2022, <https://www.defense.gov/News/News-Stories/Article/Article/3216745/400-million-security-package-headed-to-ukraine/>



- ・ 102mm榴弾砲 36 門。
- ・ HIMARS（高機動ロケットシステム）38 門
- ・ HAWK ミサイル、数未公表；NASAMS 中高度防空システム 8 式；Avenger 短距離防空システム 4 式
- ・ 各種装甲車 800 台程度；ハンヴィー高機動汎用装輪車両 1000 台以上；その他、ヘリコプター、T-72 戦車、トラック、トレーラなど各種車両；装甲医療車両 100 台。
- ・ MAXAR 社など商用衛星画像サービスの提供
- ・ 個人装備品（ヘルメット、防弾チョッキ、赤外線暗視装置、救命セット、防寒服他）

その後も、米国の軍事支援は、武器の種類も増加して継続している。2023 年 7 月 18 日の国防総省の広報資料<sup>28</sup>に拠れば、米国政府は、2022 年 2 月 24 日の全面侵攻以来同日までの間に合計 426 億ドル以上の支援を約束している。邦貨に換算すれば、6 兆円近くの巨額の支援である。更に、その武器には、精密誘導のロケット弾や砲弾など最先端の武器が含まれている。

#### ④ インテリジェンス優位

そしてウクライナ側の要因の最後が、ウクライナのインテリジェンス優位である。それは第 1 に、米国のインテリジェンス支援であり、米国は、その世界最高のインテリジェンス力を使って、ウクライナの戦争努力を全面的に支援しているのである。次に第 2 に、ウクライナ自身のインテリジェンス力であり、中でも優秀なセキュリティ・サービスによる貢献である。

それでは、これらインテリジェンス優位の実態を、これから見ていこう。

### 3 米国政府の対応に見るインテリジェンス力の現れ

今回のロシア・ウクライナ戦争において、米国インテリジェンスが如何に優れた能力を発揮して、ロシアの意図と行動を正確に把握し米国の国策に貢献しているか、全面侵攻に至るまでの米国政府の一連の行動から見てみよう。

#### （1）ロシアのウクライナ全面侵攻の予測と対応準備

米国インテリジェンスが、今次戦争に関係して如何に優れた能力を発揮しているかについては、2022 年 2 月 24 日のロシア軍全面侵攻に至る前の米国政府の動向を顧みれば明白である。他の多くの諸国がロシア軍の全面侵攻には懐疑的であった時点から、そのインテリジェンス力によって全面侵攻を予測して行動していたのである。

即ち、ロシア軍は 2021 年春季演習でウクライナ東方に数万の兵を集結してウクライナを威嚇したが、米国インテリジェンスは秋季演習では更に大規模な兵員の動員計画を把握し

<sup>28</sup> DoD, *Fact Sheet on U.S. Security Assistance to Ukraine, July 18, 2023*, accessed 25 July, <https://media.defense.gov/2023/Jul/19/2003263170/-1/-1/1/UKRAINE-FACT-SHEET.PDF>

た。その動員規模は、必要な資源量から判断しても軍事演習としては過大であり、加えて、ロシア政府は軍事作戦用予算の異常な増額や予備兵力の増強に取り組むなど、それは全面的侵攻作戦を予測させた<sup>29</sup>。

そこで、米国インテリジェンスは2021年10月初めにはその旨を大統領に報告し<sup>30</sup>、米国政府は10月27日ホワイトハウスで対応策を協議。ここで、ミリー統合参謀本部議長はロシアの作戦計画として、北・東・南の多方面からの全面同時侵攻、3、4日での首都キーウ占領、特殊部隊によるゼレンスキー大統領の排除、傀儡政権の樹立、その後更にロシア軍は西進してウクライナ国土の大部分を占領するであろうと説明した<sup>31</sup>。また、ヘインズ国家諜報長官が、ロシア軍は2022年1月末までには攻撃準備を完了すると報告し、プーチンに攻撃を思い止まらせるため元駐露大使バーンズ CIA 長官のモスクワ派遣を決定した。またその場で、ロシアの侵攻への対処計画を調整し策定するために、ホワイトハウスにプロジェクトチーム「タイガーチーム」の設置を決定した。同チームは、ロシア軍侵攻について幅広いシナリオを想定して、これらに対する外交対応、米軍の対応、情報作戦、難民問題、経済制裁、大使館警備、サイバー攻撃対処その他全分野に渉る対処計画を調整策定した<sup>32</sup>。

2021年11月2日、バーンズ長官はモスクワを訪問。ロシア大統領府クレムリンから黒海沿岸ソチに居たプーチン大統領と秘匿電話で会談した。バーンズは会談で「米国政府は、プーチンがウクライナ侵攻を計画していると考えている(believe)が、もし実行すればロシアは甚大な制裁を被ることになる」と警告した。これに対して、プーチンは軍事侵攻の可能性を否定しなかったという。バーンズ CIA 長官は、バイデン大統領に「プーチンは、最終決定はしていないものの、侵攻に強く傾いている」という評価を報告した。米国インテリジェン

---

<sup>29</sup> Michael R. Gordon, et.al., “Vladimir Putin’s 20-Year March to War in Ukraine—and How the West Mishandled It,” *The Wall Street Journal*, 1 April 2022, accessed 7 May 2022, [https://www.wsj.com/articles/vladimir-putins-20-year-march-to-war-in-ukraineand-how-the-west-mishandled-it-11648826461?mod=hp\\_trending\\_now\\_article\\_pos1](https://www.wsj.com/articles/vladimir-putins-20-year-march-to-war-in-ukraineand-how-the-west-mishandled-it-11648826461?mod=hp_trending_now_article_pos1).

--Shane Harris, et.al., “Road to war: U.S. struggled to convince allies, and Zelensky, of risk of invasion,” *The Washington Post*, 16 August 2022, accessed 18 August 2022, <https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/>

本章の記述は、他に出典を示さない限り上記の分析記事によっている。

<sup>30</sup> 小泉悠氏によれば、10月初め米国インテリジェンスはロシア軍侵攻に関するインテリジェンス報告を大統領に提出したと *The Washington Post* が報道している。「報道1930」BS-TBS、2022年10月25日放送。

<sup>31</sup> ミリー統参議長の説明の根拠は、衛星画像によるイミント、通信傍受によるシギント、そしてヒューミントであり、米国インテリジェンスはロシア政治指導部、インテリジェンス機関、軍の多数の個所から情報を得ていると説明されている。Shane Harris, et.al. *ibid*.

<sup>32</sup> 「タイガーチーム」の正式発足は11月であるが、国防総省、国務省、エネルギー省、財務省、国土安全保障省、インテリジェンス諸機関の担当者が参加した。同チームは、ウクライナに対する限定的な武力行使から、大規模侵攻によるウクライナ全土占領まで幅広いシナリオを想定して、これらに対する外交対応、米軍の対応、情報作戦、難民問題、経済制裁、大使館警備、サイバー攻撃対処その他全分野に渉る対処計画を調整策定した他、12月には閣僚も参加して模擬訓練を実施したという。Ellen Nakashima and Ashley Parker, “Inside the White House preparations for a Russian invasion,” *The Washington Post*, 12 February 2022, accessed 13 May 2022, <https://www.washingtonpost.com/national-security/2022/02/14/white-house-prepares-russian-invasion/>

スは既にこの時点でウクライナ侵攻の確度が極めて高いと評価していたのである。

米国は欧州諸国にもロシア軍侵攻について警告を始めた。特に11月17日のNATO評議会では、ヘインズ国家諜報長官が一定の情報を示してロシアによる全面侵攻の可能性について警告した。しかしこの時点では、独仏は侵攻そのものに懐疑的であり、その他の国々もせいぜい限定的侵攻であろうと想定していた。全面侵攻を信じたのは英国<sup>33</sup>とバルト三国のみだったという。

11月下旬、ウクライナ国防相レズニコフが訪米し、米国防長官等と協議したが、レズニコフ国防相がロシア軍の限定的侵攻を想定していたのに対して、米ミリー統合参謀本部議長はロシア軍の大規模侵攻を警告した。米国インテリジェンスは、ロシア軍の軍事侵攻は、ウクライナ東部に対する限定的侵攻ではなく、首都を含む大規模侵攻の可能性が高いと評価していたのである。

この訪問を受け、12月初旬、米国防総省作業チームがウクライナ訪問して、ロシア軍侵攻に備えて米国のウクライナに対する軍事支援を協議したが、協議対象は防空戦、海上戦、電子戦、サイバー戦各分野に及んだ<sup>34</sup>。また、後述するように、米サイバー軍のサイバー防禦作戦担当の部隊も同時期からウクライナに派遣されている、

## (2) 米国による情報作戦

2021年12月3日米国政府は、一部のインテリジェンスの機密指定を解除して、ロシア軍の動向を公表した。即ち、同日付けのワシントン・ポスト紙はインテリジェンス機関作成文書を報道したが、それによれば、ロシアは年明けのウクライナ攻撃を計画しており、既にウクライナ周辺4方面に大隊戦術集団50個(兵員7万人)が集結している。大隊戦術集団100個(17万5千人)の動員が可能で、キーウ占領を目的としていると予測していた。この文書は衛星写真を添付した分かり易い文書であった<sup>35</sup>。

本報道は大きな反響を呼んだが、米政府は、この情報開示による牽制の結果、開戦を2月下旬にまで遅らせることができたと考えている。また、この情報開示で、西側の結束を強化するなど対応策を準備する時間ができたのである<sup>36</sup>。米国は、この他にも多くの情報を開示

---

<sup>33</sup> 英国が全面侵攻を信じたというのは不思議ではない。英国はUKUSAシグント同盟の主要参加国であり、ロシアの戦争準備について米国と同等のシグント情報を保持していたと推定できる。

<sup>34</sup> Abraham Mahshie, "With Russia on Multiple Fronts, DOD Team in Ukraine Assesses Air Defense Needs," *Air Force Magazine*, 3 December 2021, accessed 7 May 2022, <https://www.airforcemag.com/with-russia-on-multiple-fronts-dod-team-in-ukraine-assesses-air-defense-needs/>, 2014

<sup>35</sup> Shane Harris and Paul Sonne, "Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns," *The Washington Post*, 3 December 2022, last accessed 12 May 2022, [https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad\\_story.html](https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html)

<sup>11</sup> Ken Dilanian, et.al., "In a break with the past, U.S. is using intel to fight an info war with Russia, even when the intel isn't rock solid," *NBC News*, 5 April 2022, accessed 7 May 2022, <https://www.nbcnews.com/politics/national-security/us-using-declassified-intel-fight-info-war-russia-even-intel-isnt-rock-rcna23014>

して、ロシアによるプロパガンダを阻止し正しい情勢認識を発信している<sup>37</sup>。

12月中旬に、米国は国務省欧州ロシア担当カレン・ドンフリードを訪露させ、ロシア外務次官リャブコフと交渉させた。ロシア外務省は、ウクライナのNATO非加盟の約束など強硬な条約案二つを提示し、その後一方的に公表したが、米国はこれは今後のロシア軍による侵攻作戦を正当化する作業であろうと危惧した。

以上の情勢を受けバイデン大統領は、12月27日ウクライナに対する緊急武器提供を承認した。

### (3) 侵攻開始直前の米国政府の行動

2022年1月9日、米露の外交軍事担当官がジュネーブで会談した。米国務次官シャーマンと統合参謀本部作戦部長ミンガス中將は、ロシア外務次官リャブコフとロシア軍将官と会談した。その席上、米ミンガス中將は、自分のイラクやアフガニスタンでの戦場体験から判断して、ウクライナに侵攻すれば何年にもわたる泥沼の作戦となると警告したが、ロシア側は反応を示さなかった。

この前後から、米軍はバルト三国やポーランド、ハンガリー、ブルガリア、ルーマニアなど東欧諸国への兵力配置を増強している。欧州駐留兵力を7万4千から10万人に、戦闘機部隊や艦船の配置も増やしている。また、東欧諸国からの情報偵察活動を強化している。

1月21日、プリンケン米国務長官はジュネーブでラブロフ露外相と会談して、もしロシア軍がウクライナに侵攻すれば、ロシア経済を麻痺させる経済制裁を課し、ウクライナには大規模軍事支援を行う、NATO諸国を攻撃すれば米国は参戦する、と警告を発した。

2月14日、米国は逸早くウクライナ・キーウの米大使館の閉鎖を発表した。この閉鎖発表は、他の諸国よりも早く唐突の感も否めなかったが、米国は既にロシアのウクライナ全面侵攻とキーウ占領計画を確信していたのであるから、むしろ自然な措置であろう。

### (4) 米国のウクライナに対する情報支援の恒常化

米CIAバーンズ長官の議会証言によれば、バーンズは2022年1月12日ウクライナを訪問してゼレンスキー大統領と面会し、ロシア軍の作戦計画について図解を使用して詳細な情報を提供した。そして、それ以来米国は毎日情報提供を継続してきた。つまり、ロシア軍の

---

<sup>37</sup> 米国は、西側諸国に正しい状況認識を促し、ロシアによる宣伝工作を阻止するために、情報を積極的に開示する情報作戦を多様に展開している。顕著な例をもう一つ示すと、全面侵攻前の2月上旬ロシアによる「偽旗作戦 (false frag operation) の阻止である。2月3日国防総省カービー報道官は、要旨次の様に述べた。「ロシアはウクライナ侵攻を正当化するため、ウクライナ部隊によるロシア領やロシア語話者に対する攻撃を捏造しようとしている。その為、遺体や会葬者や破壊現場を映した宣伝ビデオを作成すると見ている。」この警告発言によってロシアによる偽旗作戦の効果を減衰させ事前に抑止したのであるが、この背景には、米国インテリジェンスが現実的にロシアにおける偽旗作戦の準備動向を把握していた事実があった。DOD, *Press Briefing by Pentagon Press Secretary John F. Kirby*, 3 February 2022, accessed 1 June 2022, <https://www.defense.gov/News/Transcripts/Transcript/Article/2922998/pentagon-press-secretary-john-f-kirby-holds-a-press-briefing/>

戦争計画とロシア軍部隊の動きについて、継続的に情報を提供してきたのである<sup>38</sup>。なお1月12日の時点で、米国インテリジェンスは、ロシア軍の首都キーウ攻撃は郊外のホストメリ空港制圧を持って始まること、ゼレンスキー大統領暗殺部隊が既に首都に潜入している可能性があること、までも把握しており、これらの情報はゼレンスキー大統領とウクライナ諜報機関に伝えられた<sup>39</sup>。

この情報提供があったからこそ、キーウは侵攻数日にして陥落するという予測が一般的な中で、ウクライナが効果的に抗戦出来たのである。

元々ウクライナ軍は、ロシアの侵攻開始前の段階では、東部地方に対する限定侵攻の可能性の方が高いと判断していたが、米国から伝えられた全面侵攻の可能性も想定して作戦計画を策定していた。そのため、進攻開始時、首都キーウ北方のホストメリ空港のロシア空挺部隊による占拠を遅延させることに成功し、首都の電撃的な占領を阻止し得た。また、開戦劈頭、敵の空軍力や防空システムを破壊・無力化して、航空優勢を確保するのが戦争の常道であるが、これも阻止することができた。皆、米国によるインテリジェンス支援の効果である。

#### (5) プーチンによる核ブラフへの対応

ロシア軍の全面侵攻開始後、米国はそのインテリジェンス力を使用して、ウクライナ軍の抗戦を支援してきたが、勿論、それに留まらず米国政府自体の行動にもそのインテリジェンス力は活かされ続けている。

その典型例が、ロシアのプーチン大統領による戦術核使用のブラフに対する対応がある。

報道から判断して、米国はロシアの戦術核使用の準備行動を探知するインテリジェンス力を持っていると見られる。即ち、ロシア軍が、戦術核を使用のために移動させたり、その他（秘密の核訓練や戦略部隊のアラート態勢などの）攻撃の準備行動を探知する能力である。しかし、これらの探知能力は完全ではなく、大統領に相当事前に（much advanced）警告を発する時間的余裕までは保証は出来ないという。また、軍指導者間の協議についても一定程度把握する力を持っている。

プーチンは、開戦以来、米欧諸国を威嚇するために、戦術核兵器使用の脅しを度々かけている。開戦直後の2022年2月27日には核戦力の特別警戒態勢を命じた。更に、注目されたのは、9月21日の発言である。9月にはウクライナ軍の反攻によりハルキウ州のロシア軍が敗走し、戦況はロシアに不利に転じた。そのような状況を受け、プーチンは、部分動員令を表明した演説の中で、米国による広島長崎に対する原爆投下に言及した上で、「ロシア領土に対する脅威に対抗するためにはあらゆる手段を講じる。これはブラフではない」旨述

---

<sup>38</sup> CIA Director Burns, *Hearing on Annual Worldwide Threats before Permanent Select Committee on Intelligence*, U.S. House of Representatives, Washington, D.C., 8 March 2022, <https://docs.house.gov/meetings/IG/IG00/20220308/114469/HHRG-117-IG00-Transcript-20220308.pdf>

<sup>39</sup> Shane Harris, et.al., “Road to war: U.S. struggled to convince allies, and Zelensky, of risk of invasion.”

べた<sup>40</sup>。ロシアが併合手続に入ったドネツク、ルガンシクなど4州の保持のために核兵器使用があり得ることを匂わせたのである。

これに対して、サリバン米大統領安全保障担当補佐官が、9月28日には、「核兵器の使用は、ロシアに破滅的な結果をもたらす。仮にロシアが使用すれば、米国とNATO諸国がどう対処するかは伝えてある」旨を述べ、米国は核兵器を使用しないように警告を発していることを明らかにした<sup>41</sup>。

更に、10月にはオースチン国防長官がショイグ国防相と21日23日と連続して電話会談を行った。両者の電話会談は5月以来であり、且つ2回連続したことで注目された。

この会談の背景には米国インテリジェンスがあると見られる。ニューヨーク・タイムズ紙<sup>42</sup>によれば、10月中旬の情報報告で、ロシアの高級軍指導者が最近ウクライナでの戦術核のありうべき (might) 使用の時期と方法について話し合った (conversation) というものがある。オースチン国防長官とショイグ国防相の電話会談の内容については、ウクライナの状況について話し合ったというだけで、それ以上の情報は開示されていないが、米国防長官が警告を発するために会談したと推定できる。

このように、プーチンの核使用ブラフへの対応でも、米国インテリジェンスは基礎となる情報を提供しているのである。

## (6) 米国インテリジェンスの限界

上記のように、米国はその優れたインテリジェンス力を活かして、ロシア軍のウクライナ全面侵攻を前提に外交的軍事的対応をしてきた。米国のインテリジェンス力は、独仏などを遙かに上回る優れたものであった。また、例えばロシアによる戦術核使用の威嚇に対しても適切に対応している。しかし、米国インテリジェンスも万能ではない。

つまりロシア・ウクライナ戦争における米国インテリジェンスには限界も見られる。それは、CIAは大統領にロシア軍は即座に勝利するだろうと報告していたという。即ち、ロシア軍はウクライナ軍を圧倒し数日で勝利する。首都キーウの陥落は1週間以内、最長でも2週間以内。ウクライナの敗残兵ができる抵抗はせいぜい占領軍に対するゲリラ戦くらいと評価していたという<sup>43</sup>。

---

<sup>40</sup> Institute for the Study of War, “RUSSIAN OFFENSIVE CAMPAIGN ASSESSMENT, SEPTEMBER 21,” *UKRAINE CONFLICT UPDATES*, 21 September 2022, accessed 5 November 2022, <https://www.understandingwar.org/backgrounder/ukraine-conflict-updates>

<sup>41</sup> David E. Sanger, Anton Troianovski and Julian E. Barnes, “Putin’s nuclear threats stir growing alarm in Washington,” *The New York Times*, 2 October 2022, accessed 5 November 2022, <https://www.japantimes.co.jp/news/2022/10/02/world/putin-nuclear-threats-us-worry/>

<sup>42</sup> Helene Cooper, Julian E. Barnes and Eric Schmitt, “Russian Military Leaders Discussed Use of Nuclear Weapons, U.S. Officials Say,” *The New York Times*, 2 November 2022, accessed 2 November 2022, [https://www.nytimes.com/2022/11/02/us/politics/russia-ukraine-nuclear-weapons.html?campaign\\_id=60&emc=edit\\_na\\_20221102&instance\\_id=0&nl=breaking-news&ref=cta&regi\\_id=189263598&segment\\_id=111763&user\\_id=784c7a7d37c1ab1c05d5af4534d46768](https://www.nytimes.com/2022/11/02/us/politics/russia-ukraine-nuclear-weapons.html?campaign_id=60&emc=edit_na_20221102&instance_id=0&nl=breaking-news&ref=cta&regi_id=189263598&segment_id=111763&user_id=784c7a7d37c1ab1c05d5af4534d46768)

<sup>43</sup> James Risen, Ken Klippenstein, “The CIA Thought Putin Would Quickly Conquer Ukraine.

この情勢評価は米国政府の行動とも合致する。米国政府は、先にも述べた通り 2022 年 2 月 14 日にキーウの米国大使館の閉鎖を発表したが、これもキーウ占領を予想していたからであろう。また、全面侵攻前には、米国からの武器供与は主としてジャベリンやステインガーなど個人が携行できる武器に限られており、HIMARS や 155 ミリ榴弾砲などの重火器は供与しなかった。これも、ウクライナ軍が敗北すると予想していたためであろう。敗北の場合ロシア軍に鹵獲されるような重火器は供与せず、ゲリラ戦に使用できる個人携帯武器を供与したのである。

このような情勢判断の間違いが生じた理由は、米国インテリジェンスがウクライナ軍の士気と戦闘意欲を過小評価していたことに加え、ロシア軍の持つ本質的な弱体さを把握できていなかったためとされる。それはプーチン体制、特に軍部と軍需産業に蔓延する腐敗と無能・欺瞞の重要性である。腐敗と無能・欺瞞のために、指揮機構は弱体、兵員は訓練不足で、士気は低く、ロシア軍は空洞化していたのである。全面侵攻して実際の戦争で露呈して米国も初めて認識したのである。友好国の兵士の士気というような情報は正にヒューミントが担うべき情報であるが、米国インテリジェンスでは、シギント、イミント、マシントなどいわゆる技術的インテリジェンス（テキント）の分野は優れているが、CIA が担うヒューミント分野は相対的に弱体であると言われている<sup>44</sup>。

こういう事例があると、米国では相対的に弱体なヒューミント強化の議論が巻き起こり、それに影響されて我が国でもヒューミント強化の必要性が議論されることが多い。例えば 9・11 同時多発テロの際もそうであった。米国でヒューミント強化の議論が巻き起こる背景には、米国のシギント、イミントなどの技術的インテリジェンス（テキント）の能力の高さがある。そこで、ヒューミントにおいても同レベルのインテリジェンスを期待する向きが強く、その期待が満たされない時にヒューミント強化の議論が巻き起こるのである。しかし、我が国に必要なのは、先ず米国インテリジェンス力を支えるテキントの実態を知ることである。それをこれから概観してみよう。

## 4 米インテリジェンス諸機関の情報収集力の骨格

今まで見てきた米国の優れたインテリジェンス力を構成する諸機関と情報収集手段は、何であろうか。CIA のヒューミントであろうか。勿論ヒューミントも重要ではあるが、ロシア・ウクライナ戦争における米国インテリジェンスの中核は、それ以上にシギント、イミント、マシントであり、インテリジェンス機関としては、国家安全保障庁 NSA、国家地理空間諜報庁 NGA、国防諜報庁 DIA なのである。それは 2023 年 4 月に発覚した米空軍州兵テシェイラによる漏洩情報でも明らかである。漏洩情報の諜報源を見ると、シギント情報が圧

---

Why Did They GET It So Wrong?" *The Intercept*, 6 October 2022, 10 October 2022, <https://theintercept.com/2022/10/05/russia-ukraine-putin-cia/>

<sup>44</sup> Ibid.

倒的多数を占め、それに次ぐのがイミント情報であった<sup>45</sup>。

米国は、シギント、イミント、マシントそれぞれの分野で世界を覆う壮大なデータ収集網を、第二次世界大戦後に膨大な資金と人材を投入して構築してきた。これら諸機関が如何に巨大な情報収集力を有しているか、その収集プラットフォームを簡単に見てみよう。

### (1) シギント・プラットフォーム<sup>46</sup>

米国の国家シギント機関である国家安全保障庁 NSA (National Security Agency) は、英加豪ニュージーランドと UKUSA シギント同盟を結成して全世界を覆うデータ収集網を構築している。本同盟は、第二次世界大戦中のシギント協力関係を発展させたもので、現在ではこれら諸機関は一体的に機能していると思われる。米国の主要収集プラットフォームは次の通りであるが、更に英加豪 NZ のプラットフォームからの収集データも統合して分析されている。

#### ①「プリズム」計画 (Downstream)

米国の情報通信企業のデータセンターから必要データを入手するもの。協力企業は、マイクロソフト、ヤフー、グーグル、フェイスブック、パルトーク、ユーチューブ、スカイプ、AOL、アップルの 9 社である。G メール、ヤフー・メール、ホットメールなどにアクセス可能である。仮に、これらのフリーメールを使用するロシア高官がいれば、NSA はそれを入力し分析できるのである。

テシェイラ漏洩情報によれば、今次ウクライナ戦争に関して米国内で収集しているロシアやウクライナの情報も存在しており<sup>47</sup>、「プリズム」計画による収集が考えられる。

#### ② 通信基幹回線 (Upstream)

約 20 の計画により、世界のインターネット通信基幹回線の主要ポイントで、関係国の協力を得て或いは関係国に秘匿して、データを収集している。2013 年のスノーデン漏洩資料によれば、欧州では英仏独のほか、デンマーク、スウェーデン、ポーランドでも収集していた。現在ではウクライナでも収集している可能性がある。これによりロシア人の海外とのインターネット通信の一部は捕捉されている。

#### ③ 外国通信衛星の傍受 (FORNSAT)

世界の主要基地 12 箇所と次に述べる SCS (特別収集サービス) 約 40 箇所で見集めている

<sup>45</sup> 拙著『Teixeira 漏洩情報に見る米国インテリジェンス力』(警察政策学会資料第 129 号、2023 年) 参照。

<sup>46</sup> ここでは特に記述しない限り、茂田忠良『米国国家安全保障庁の実態研究』(警察政策学会資料第 82 号、2015 年) に拠っている。

<sup>47</sup> 2023 年 4 月の NSA 幹部の発言によれば、大統領への毎日の情報ブリーフィングの諜報源で、対外諜報監視法 FISA702 条に基づく収集情報が一部でも含まれている比率は 59% である。対外諜報監視法 702 条に基づく収集とは、①「プリズム」計画の全部と②通信基幹回線収集の一部であり、その重要性が理解できる。同時にそれだけで 59% を占めるということは、他のソースを含むシギント全体が大統領ブリーフィングに一部でも占める割合は更に大きいということである。

Dustin Volz, "NSA Chief Paul Nakasone Has Said He Expects to Step Down in Coming Months," *The Wall Street Journal*, 11 May 2023, last accessed 28 July 2023, <https://www.wsj.com/articles/nsa-chief-paul-nakasone-has-said-he-expects-to-step-down-in-coming-months-7c21681f>



る。これによりロシアの衛星通信の一部は捕捉されている。

#### ④ 特別収集サービス (SCS : Special Collection Service)

NSA と CIA による共同事業であり、世界の米国大使館や領事館 80 箇所以上を拠点として収集している。モスクワ、キーウ、バクー、トビリシなど旧ソ連邦諸国にも収集拠点を設定していた。モスクワ市内の通信の一部は捕捉されている。

#### ⑤ CNE (コンピュータ・ネットワーク工作)

いわゆるハッキングによる収集である。インターネット回線を通じて侵入する「遠隔侵入」と、製品供給網工作や建造物侵入などを伴う「近接侵入」の 2 種類がある。「近接侵入」には米国外での作戦に従事する専門組織も存在する。侵入したシステムは 2013 年末時点ですら既に 10 万箇所近くと推定されている。

前進防禦 (Defend Forward) をするには、CNE によってハッカー集団のシステムに先制的に侵入して彼らの攻撃意図や方法を解明することが必須である。NSA や米サイバー軍はロシアのハッカー集団のシステムをハッキングしていると推定できる。

#### ⑥ シギント衛星・機上収集 (Overhead) <sup>48</sup>

シギント衛星やシギント航空機によるデータ収集で次の収集がある。

- ・ 赤道上静止衛星：テレメトリー信号収集。マイクロ波多重通信、  
携帯電話や無線通信などを収集
- ・ 長楕円モルニア軌道衛星
- ・ 低軌道エリント衛星：レーダ波などから艦船その他の所在地を探知  
(なお、米国の民間商用衛星企業 HawkEye360 は、地上の発信電波を探知するエリント衛星を運用しているが、ロシア軍の GPS ジャミング電波を探知して発信地を捕捉して公表している。この会社も米国政府の勸奨を受けてウクライナを支援していると考えられる。テシェイラ漏洩情報によれば、米国インテリジェンス自体が、地上からの発信電波を分析して、ロシア軍の配置や動静を探知している。)
- ・ RC135 機上収集：NSA の運用する総合シギント機。今次戦争では、ウクライナに隣接するポーランド、ルーマニア、黒海上空で情報収集している。英国も RC135 を所有しており情報収集に使用しているが、2022 年 9 月 29 日に黒海上空でロシア空軍機にミサイルを発射された<sup>49</sup>。テシェイラ漏洩情報によれば、同 RC135 は、ロシア戦闘機と地上管制局管の通信も傍受していた。
- ・ 海軍 EP-3E、陸軍 RC-12、EO-5C/ARL-M などの各種シギント機があり、無線通信の

---

<sup>48</sup> Jeffrey Richelson, *the US Intelligence Community 7th ed.*, (Boulder, CO: Westview Press, 2016), pp228-241.

--Duncan Campbell, *Interception Capabilities 2000*, (Edinburgh, Scotland: IPTV Ltd, April 1999), accessed 12 June 2022, [https://balkania.tripod.com/resources/military/ic2000/ic2kreport.htm#\\_Tbc448565533](https://balkania.tripod.com/resources/military/ic2000/ic2kreport.htm#_Tbc448565533)

<sup>49</sup> James Gregory, "Russian jet released missile near RAF aircraft over Black Sea," *BBC News*, 20 October 2022, accessed 21 October 2022, <https://www.bbc.com/news/uk-63327999>

ミサイル発射は情報収集妨害の威嚇のためと見られるが、ロシアは空軍機の技術故障のための発射と言いつづけている。

傍受や地上レーダの探知特定能力を有する。更に **RQ-4 Global Hawk**、**MQ-9 Reaper** など無人偵察機はシグント収集機能を付加されている。

2023年3月14日米軍の無人偵察機 **MQ-9** は、黒海上空で情報収集中、ロシア軍戦闘機が後部プロペラに接触したため海中に落下した<sup>50</sup>。

これらの収集力によって、ロシア国内の通信の一部は捕捉されている。また、レーダを使用する軍事装備（例えば艦船、地对空ミサイル、対空機関砲）の種類と位置の捕捉が可能である。

#### ⑦ 水上艦艇・潜水艦収集<sup>51</sup>

米国は水上艦艇や攻撃型原子力潜水艦の一部にシグント収集システムを搭載して運用している。今回のウクライナ戦争では、黒海海域には米艦艇は所在していないと報道されているので、黒海では運用されていないと見られる。

#### ⑧ 従来型収集 (Conventional)

主として HF 波などの無線通信の傍受。20 世紀にシグントの中心であった。

それでは、上記のシグント・プラットフォームで収集したシグント・データの分析から何が分かるのであろうか。勿論、その実態は極秘事項であり、公刊資料からは把握し難い。しかし、**テシェイラ**漏洩情報から確実なのは、ロシアの国防省など軍事指揮機構や **GRU**、**FSB**、**SVR** などのインテリジェンス諸機関、更には民間軍事会社 **ワグネル** の通信の少なくとも一部は傍受解読していることである。また、暗号解読 (crypto-analysis) できない通信でも、通信状況分析 (traffic analysis という確立された分析手法)、或はエリント信号分析などの分析手法を使うことによって、ロシア軍の部隊編成や所在地、動向について、相当正確に把握していると考えて間違いない。

---

<sup>50</sup> 米軍の **MQ-9** 無人偵察機は、2023年3月頃はルーマニア国内の基地を拠点に毎日 9~10 時間、黒海上空を飛行して情報収集活動を行っていた。同月 14 日も定期収集に出発したが、クリミア半島南西 120 キロの地点でロシア軍 **ミグ 27** 戦闘機 2 機が飛来して、3~40 分に亘りジェット燃料を浴びせたり前方飛行するなど飛行妨害行為をしていたが、中欧時間午前 7 時頃、**MQ-9** の後尾のプロペラに接触した。**MQ-9** はプロペラ損傷により飛行継続が困難と判断されたため、米軍は海中に落下させた。他方、ロシアは接触を否定したため、米軍は **MQ-9** からの映像記録を公開した（映像には、ロシア機による妨害行為と損傷したプロペラが映っている）。飛行空域から判断して、水没した **MQ-9** はイミント・センサーよりもシグント・センサーに力点があったものと推定される。

—DOD, *Pentagon Press Secretary Brigadier General Pat Ryder and PTDO DUSD(Policy) Dr. Mara Karlin Hold a Press Briefing*, 14 March 2023, accessed 16 March 2023, <https://www.defense.gov/News/Transcripts/Transcript/Article/3329354/pentagon-press-secretary-brigadier-general-pat-ryder-and-ptdo-dusdpolicy-dr-mara/>

--Eric Schmitt and Helene Cooper, "Pentagon Releases Video of a U.S. Drone's Encounter With Russian Jets," *The New York Times*, 16 March 2023, accessed 16 March 2023, <https://www.nytimes.com/2023/03/16/us/politics/russia-drone-black-sea.html>

--Matthew Mpoke Bigg, "The U.S. European Command says the drone was downed after a Russian aircraft stuck its propeller," *The New York Times*, 14 March 2023, accessed 15 March 2023, <https://www.nytimes.com/live/2023/03/14/world/russia-ukraine-news>

<sup>51</sup> Richelson, pp.251-254.

なお、2015年にウィキリークスが報じたNSA漏洩情報<sup>52</sup>から判断して、当時、米国NSAはフランスやドイツの大統領、首相、有力閣僚など政府高官の暗号化電話通信を傍受解読していた。また、日本の首相の動静についても機微な情報が捕捉されていた。このような通信傍受努力は米国の同盟諸国に向かっているだけではなく、当然、ロシアに対してはより強く向けられている。プーチン大統領は、元KGB将校であり、ウィキリークス漏洩情報は熟知している筈であるから、プーチン自身の電話通信が傍受解読されていることはないであろうが、より低いレベルの職員ともなれば、必ず隙が生じるものである。プーチンは、それを知っているからこそ、ウクライナ全面侵攻の決断を部下に周知するのを間際に至るまで控えたのであろうが、皮肉にも、それがロシア軍全面侵攻の準備不足をもたらしたのであろう。

## (2) イミント・プラットフォーム<sup>53</sup>

米国の国家イミント機関である国家地理空間諜報庁NGA (National Geospatial-Intelligence Agency) は、2009年に英加豪NZのイミント諸機関とASG (Allied System for Geospatial Intelligence) を結成した。このASGはイミント版UKUSA同盟とでもいうべきもので、米国のみならず、英加豪NZのイミント資産も総合して運用しようとするものである。米国の主な収集プラットフォームは次の通りであるが、更に英加豪NZのプラットフォームからの収集データも統合して分析されていると見て間違いはない。

これらの収集プラットフォームを総合的に運用することで、ロシア軍の部隊、装備や所在地について、正確な情報を把握することが可能である。

### ① 国家衛星システム

- ・ デジタル光学衛星KH-11シリーズ：極めて高解像度で広域撮像が可能。
- ・ レーダ衛星ONYXシリーズ：曇天、夜間でも撮像可能。ウクライナは冬季曇天が多く、また、ロシア軍は秘匿のため軍部隊移動に夜間を好む傾向があり、レーダ衛星の価値が高いと言われる。

カナダもレーダ衛星を運用しているが、そのデータはASGの枠組で米国も利用していると考えられる。

---

<sup>52</sup> NSA漏洩資料、“Top French NSA Intercepts,” *WikiLeaks*, 23 June 2015, accessed 24 June 2015, <https://www.wikileaks.org/nsa-france/intercepts/>

-- NSA漏洩資料、“Top French NSA Targets,” *WikiLeaks*, 23 June 2015, accessed 24 June 2015, <https://wikileaks.org/nsa-france/selectors.html>

-- NSA漏洩資料、“Top German NSA Intercepts,” *WikiLeaks*, 20 July 2015, accessed 21 July 2015, <https://www.wikileaks.org/nsa-germany/intercepts/>

-- NSA漏洩資料、“Top German NSA Targets,” *WikiLeaks*, 20 July 2015, accessed 20 July 2015, <https://wikileaks.org/nsa-germany/selectors.html>

-- NSA漏洩資料、“Top Japanese NSA Intercepts,” *WikiLeaks*, 31 July 2015, accessed 3 August 2015, <https://www.wikileaks.org/nsa-japan/intercepts/>

-- NSA漏洩資料、“Top Japanese NSA Targets,” *WikiLeaks*, 31 July 2015, accessed 3 August 2015, <https://www.wikileaks.org/nsa-japan/selectors.html>

<sup>53</sup> Richelson, pp184-212.

## ② 米国商用衛星<sup>54</sup>

- ・ MAXAR 社の WorldView など 4 機：高解像度。米 NGA と基本契約を結んでおり、公式非公式の撮像統制が及んでいる。純然たる民間企業と言うよりも、NGA の別動隊と理解すべきである。画像が市販可能なので、米国が同盟国と情報を共有する際に有用な媒体となっている。米国防総省の広報によれば米国政府の資金援助を得てウクライナ政府には無制約で提供されていると考えられる。また商用衛星画像に、国家衛星システムなどの情報分析を付加することで、より高度の分析情報を共有できる。

テシェイラ漏洩情報によれば、米国インテリジェンスは、精密誘導弾を使用したウクライナ軍によるロシア軍攻撃の効果測定や損害評価に、国家衛星情報と共に米国商用衛星の画像を使用している。

- ・ 他に Planet Labs、BlackSky Technology などの新興商用衛星企業も、米国政府の勧奨を受けてウクライナに協力していると考えられる。

## ③ 有人偵察機

- ・ U-2 偵察機、P-8 偵察機：光学画像、レーダ画像の撮像可能

## ④ 無人偵察機

- ・ RQ-4 Global Hawk：光学、レーダ画像の他、シグント能力もある。
- ・ RQ-170 センチネル、RQ-180 ステルス機：探知困難な偵察機
- ・ プレデター・シリーズ：無人攻撃機として有名であるが、イミント機能もある。

今回の戦争では、U-2 偵察機、RQ-4 Global Hawk や MQ-9 Reaper が、ウクライナ隣接の NATO 諸国に配置されて、情報収集に当たっている。

なお、NGA 長官は 2022 年 4 月 25 日公開の席で、NGA は米国の商用画像衛星会社に対してウクライナ支援を推奨していると述べた。また、NGA 自体の協力例として、3 月に ARTEMIS と称する戦術用・空中偵察映像地図化システムの使用方法の訓練を施したことを明らかにした。本システムは、作戦用の地理空間情報の処理システムで、小型ドローンで撮った映像から敵軍の部隊の正確な位置情報を地図化することができる。天候が悪い時でも使用可能なものである<sup>55</sup>。

## (3) マシント・プラットフォーム

マシントとは計測・特徴諜報のことであり、対象の物理的表象を計測して特徴を分析することによって得る諜報活動であり、国防諜報庁 DIA(Defense Intelligence Agency)の所掌である。具体的には、各種ミサイルの発射探知、核実験の探知、戦略原子力潜水艦・攻撃型原潜の探知その他核戦力に係わるものに力点が置かれてきたが、それに限られない。

収集プラットフォームとしては、早期警戒衛星、海上ミサイル追跡艦、各種の地上レー

<sup>54</sup> “Ukraine: The New Satellite War – Digital Eye,” *NHK World*, 15 July 2022, accessed 17 July 2022, <https://www.youtube.com/watch?v=ahbnVYro1G8> 参照。本番組では、光学画像衛星、レーダ画像衛星、電波探知衛星の機能についての基本的説明がなされている。

<sup>55</sup> Nathan Strout, “How one US intelligence agency is supporting Ukraine,” *C4ISR*, 26 April 2022, accessed 11 May 2022, <https://www.c4isrnet.com/intel-geoint/2022/04/25/how-one-us-intelligence-agency-is-supporting-ukraine/>

ダ、海中固定ソナー、音響観測艦、対潜水艦哨戒機など、様々なものがある。

ウクライナ戦争との関係では、報道はされていないが、ロシア軍による各種ミサイル発射は、米国のミサイル探知用の早期警戒システムによって、相当部分が探知され、ウクライナ軍に通報されているのではないかと推定される。

また、E-3 Sentry 早期警戒機 AWACS のウクライナ隣接 NATO 諸国への配備が報道されている。これはロシア軍航空機やミサイルの飛行捕捉に使用されていると考えられる。

以上述べたように、米国のインテリジェンス力の背景には、このようなシグント、イミント、マシントの総合力がある。これらインテリジェンス力の構築は、米国が戦後長期間に亘り膨大な資金と人材を投資してなし得たものであり、他国が一朝一夕に真似し得るものではないのである。

## 5 米国によるインテリジェンス支援

次に、今回の全面侵攻後のウクライナに対する米国のインテリジェンス支援について述べる。

既述のように、米国はバーンズ CIA 長官が 2022 年 1 月 12 日にウクライナを訪問して、ゼレンスキー大統領と面会し、ロシア軍の対ウクライナ作戦計画について図解を使用して詳細に情報を提供した。そして、それ以来毎日情報提供を継続してきたのである。

### (1) 情報提供方針・提供情報内容

#### ア 初期の情報提供方針（提供内容）

情報提供方針は、2022 年 3 月 3 日大統領府サキ報道官が説明している。即ち、「ここ数か月に亘り、ロシア軍の諸計画と諸活動について相当量のインテリジェンスを詳細且つ迅速にウクライナ政府に提供してきた。」「これには、ロシアの侵略に対し、軍事的対抗措置を講ずるのに使用できる情報が含まれている。」「情報はリアル・タイムで提供している。」と発言している<sup>56</sup>。

つまり、1 月の CIA 長官のウクライナ訪問以来継続的にインテリジェンス支援をしているということであり、具体的な提供情報は、ロシア軍の活動と位置情報、そして作戦計画に関する情報である<sup>57</sup>。作戦に使える（actionable な）情報を提供しているのである。

---

<sup>56</sup> White House, *Press Briefing by Press Secretary Jen Psaki*, 3 March 2022, accessed 5 May 2022, <https://www.whitehouse.gov/briefing-room/press-briefings/2022/03/03/press-briefing-by-press-secretary-jen-psaki-march-3rd-2022/>

<sup>57</sup> Natasha Bertrand and Katie Bo Lillis, “US officials say Biden administration is sharing intelligence with Ukraine at a 'frenetic' pace after Republicans criticize efforts,” *CNN News*, 4 March 2022, 14 April 2022,

<https://edition.cnn.com/2022/03/04/politics/us-ukraine-intelligence/index.html>

## イ 情報提供の拡大

情報提供方針は、侵攻当初は首都キーウ防衛を中心に定められていたが、3月にはロシア軍が首都占領を断念して、当面の目標をウクライナ東南部の占領併合に変更した。そこで、ウクライナ側としては東南部の占領拡大の阻止・占領地の回復が課題となった。ところで、キーウ北方は森林が多く地形からしても比較的接近した戦闘が重要であった。他方、東南部は平原が多く遠距離からの砲撃戦が重要となり、それに適したインテリジェンス支援が必要となった。

そこで、米国防長官は、4月7日頃、情報提供範囲を拡大する新方針を策定したが、新方針は、占領されたウクライナ領土の回復に（即ち、ウクライナ軍の攻勢に）資する情報を提供することを明確にした<sup>58</sup>。東南部で重要となる砲撃戦、ドローン攻撃や兵站線に対する攻撃に資する情報であろう。

## ウ 情報提供の制限の考え方

それでは、米国は無制限に情報を提供しているのでしょうか。

勿論、そんなことは有り得ない。米国がウクライナ政府に知らせたくないインテリジェンス手法と諜報源については当然開示されない。

それに加えて、米国自身が戦争当事国（参戦国）と見做されるような形ではインテリジェンスの提供はしない。つまり、インテリジェンス支援によって、米軍がウクライナ軍の作戦を指揮したり、共同で軍事作戦を実施していると見做されるようなインテリジェンス提供はしないという事である。

ここで参考とされているのが1986年の国際司法裁判所判決であるとされる<sup>59</sup>。本事件はニカラグア内乱における米国の介入の違法性、反政府勢力コントラに対する米国の支援の違法性が争われたものである。判決<sup>60</sup>では、コントラによる幾つかの作戦は、米国アドバイザーが計画実行したものではなかったとしても、少なくとも米国アドバイザーの密接な協力の基に、且つ米国のインテリジェンスと兵站の支援の基に、計画実行されたものであり、これはニカラグアの主権を侵害しており、国際法に違反するとされた。

本判決から類推すれば、米国がウクライナに対して膨大な武器その他の支援をしていることは公知の事実であり、更にインテリジェンス支援によって、実質的に米国がウクライナと共同で軍事作戦を実施していると見做される状態は回避しようとしていると見られる。

その典型が「標的情報」であり、米国政府は「標的情報」は提供していないとしている。

---

<sup>58</sup> DOD, *Press Briefing by Pentagon Press Secretary John F. Kirby*, 8 April 2022, accessed 26 May 2022, <https://www.defense.gov/News/Transcripts/Transcript/Article/2994994/pentagon-press-secretary-john-f-kirby-holds-a-press-briefing/>

<sup>59</sup> Natasha Bertrand and Katie Bo Lillis, “Biden administration walks fine line on intelligence-sharing with Ukraine,” *CNN News*, 4 March 2022, accessed 14 April 2022, <https://www.nbcnews.com/news/investigations/biden-administration-walks-fine-line-intelligence-sharing-ukraine-rcna18542>

<sup>60</sup> International Court of Justice, *Nicaragua v. United States of America, Case concerning military and paramilitary activities in and against Nicaragua, Judgment of 27 June 1986*, p.51, pp.136-137, accessed 20 April 2022, <https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf>

つまり、米国はあくまでインテリジェンス支援を行っているだけであり、ウクライナは自分の収集情報と統合して、自己の判断で攻撃をしているのであって、米国がここを攻撃せよとか、攻撃したら良いとか、を指定した情報は提供しないということである。

以上を要約すると、「標的情報 (targeting intelligence)」自体は提供していないが、作戦に使用可能な (actionable) 戦場の情報 (battlefield intelligence) は提供しているというのが米国政府の立場である。

## エ 提供禁止情報

上記の考え方の下、次の情報は提供が禁止されていると報道されている<sup>61</sup>。

- ロシア領内の攻撃のための支援情報
- ロシア軍の将軍の位置探知情報 (将軍を殺害するための位置情報は提供しない。但し、ロシア軍司令部の位置情報を提供した結果、ウクライナ軍の判断で司令部を攻撃するのは自由)
- ロシア指導部 (ゲラシモフ参謀長、ショイグ国防相等) を殺害するための支援情報

## (2) インテリジェンス支援の方法

### ア 情報提供の窓口

米国政府では、国家諜報長官室がウクライナとの情報共有指針全般を作成し、それに基づき、国防長官室が同指針の軍事作戦関連の実施方法を決定することとなっている<sup>62</sup>。

戦争遂行のための対ウクライナ支援情報は、米国諸インテリジェンス機関がそれぞれ個別にウクライナ側に提供するのではなく、米欧州軍司令部 EUCOM を通じて一元的に提供されていると報道されている<sup>63</sup>。欧州で米軍が軍事作戦を行う際の仕組みを使い、それに提供情報のスクリーニングを掛ける方式であり、合理的である。

### イ 提供する情報形態

提供する情報形態は、基本的に、情報成果物であり、諜報源や入手方法が分かる情報は提供していない<sup>64</sup>。即ち、シギントやイミントやマシントの素データそのものは提供していないということである。

但し、商用衛星画像サービスの提供は米国政府公表資料にも明記されており<sup>65</sup>、MAXAR

<sup>61</sup> Shane Harris and Dan Lamothe, "Intelligence-sharing with Ukraine designed to prevent wider war," *The Washington Post*, 11 May 2022, accessed 12 May 2022, <https://www.washingtonpost.com/national-security/2022/05/11/ukraine-us-intelligence-sharing-war/>

<sup>62</sup> Michael R. Gordon, Warren P. Strobel and Vivian Salama, "Biden Administration to Provide Ukraine With More Intelligence, Heavier Weapons to Fight Russia," *The Wall Street Journal*, 13 April 2022, accessed 15 May 2022, <https://www.wsj.com/articles/u-s-expands-flow-of-intelligence-to-ukraine-as-white-house-sends-more-arms-11649868029>

<sup>63</sup> Ken Klippenstein and Sara Sirota, "U.S. Quietly Assists Ukraine with Intelligence, Avoiding Direct Confrontation with Russia," *The Intercept*, 18 March 2022, accessed 12 April, <https://theintercept.com/2022/03/17/us-intelligence-ukraine-russia/>

<sup>64</sup> Ibid.

<sup>65</sup> 例えば、Department of State, *FACT SHEET: U.S. Security Cooperation with Ukraine*, 24 May 2022, accessed 26 May 2022, <https://www.state.gov/u-s-security-cooperation-with-ukraine/>

Technologies 社など米国商用衛星については、データを含めて多量の画像が提供されている。米国商用衛星に対しては米国の国家地理空間諜報庁 NGA の統制が及んでおり、市販されていない画像についてもウクライナ政府はアクセスを認められていると推定できる。

作戦に使える情報が主体であるので、商用衛星画像に米国の国家衛星画像、シグント情報その他で分析した成果を付加したものの提供が多いのではないかと考える。

## ウ 提供方法

全面侵攻前に、米国は、ウクライナ軍と米欧州軍司令部間に直接通信を開設した。情報の提供方法は、当初は秘匿通信装置を使っていたが、開戦直後に停電や回線不良で障害が発生したとされる。そのため、秘匿ポータルサイトに情報を掲示しそれをウクライナ側からアクセスする方法を取ったと報道されている<sup>66</sup>。その後、首都キーウ周辺の状況が安定したので、再び、秘匿通信装置を使用した提供に戻ったと推定できる。

### (3) インテリジェンス支援の成果

既述の通り、米国によるインテリジェンス支援があったからこそ、首都キーウは侵攻数日にして陥落するという予測が一般的な中で、ウクライナがこれを阻止するなど効果的に抗戦出来ているのである。

インテリジェンス支援としては、ロシア軍の作戦計画、部隊の規模・位置・進行方向などの基本的情報が提供されていれば、適切な防衛作戦計画の立案が可能であり効果的な抗戦が行われ得たことは、想像に難くない。

2022年2月ロシア軍の侵攻前の時点では、ウクライナは、米国からの全面侵攻の警告にも拘わらず、東部地方に対する限定侵攻の可能性の方が高いと判断していた。それは、侵攻2日前のレズニコフ国防相との電話協議で、ベラルーシのクレニン国防相が「ベラルーシ側からの侵略はあり得ない」と確約したこと<sup>67</sup>、や、ベラルーシ国内のロシア軍の戦闘準備が不十分であることを把握していたことなどのためであろう。しかし、それでも、ウクライナ軍統合軍司令部ではロシア軍の全面侵攻に対する作戦計画も立案されていたのである<sup>68</sup>。また侵攻開始後も、ロシア軍の動向に関する情報が提供されているため、全面侵攻に対する首都防衛で、待伏せ攻撃などの抗戦を効果的に実施することができたのである。

インテリジェンス支援の効果が具体的に報道されている事象には次のものがあるが、これらは、戦況に影響を与える重要な事件であった。

## ア ホストーメリ空港における激戦（侵攻当初）

ロシアの戦争計画では、侵攻直後に首都キーウ北西のホストーメリ軍用空港をヘリボーン部隊によって急襲占拠して、ここを作戦拠点に兵力を空輸増強し、数日の内に首都制圧を図

<sup>66</sup> Natasha Bertrand and Katie Bo Lillis, “US officials say Biden administration is sharing intelligence ....”

<sup>67</sup> 「NHKスペシャル『ウクライナ大統領府 軍事侵攻・緊迫の72時間』NHK、2023年2月26日放送。

<sup>68</sup> Daniel Michaels, “The Secret of Ukraine’s Military Success: Years of NATO Training.”



る予定であった。ところが、ウクライナは攻撃予測の情報提供を受けていたためこれを邀撃して激戦となった。ロシアの精鋭部隊である空挺部隊は一旦着陸したもののウクライナ軍の砲撃や航空機による爆撃を受け大打撃を被った<sup>69</sup>。相当数のヘリコプターも破壊された<sup>70</sup>。結局ロシア軍は同空港を占拠したものの占拠に時間を要し大損害を被り、計画通りの作戦を実現できなかった<sup>71</sup>。もし侵攻直後にロシア空挺部隊が空港を計画通り短時間で占拠できていれば、戦況は大きく変わっていたであろう。インテリジェンス支援の重要性を示す好例である。

なお、ウクライナのクレバ外相は、全面侵攻開始数日前にワシントン DC を訪問したが、そこでは、「ロシアの A 空港には、現在、輸送機 5 機が何時でも空挺部隊員を搭乗させて離陸できる状態で待機中であり、目的地はウクライナの B 空港である」とブリーフィングを受けている<sup>72</sup>。B 空港とはホストーメリ空港である。

### イ 兵力温存とロシア軍の航空優勢の阻止（侵攻当初）

開戦劈頭では、ミサイルや航空機による先制攻撃によって、敵の空軍力や防空システムを無力化して、航空優勢を確保するのが戦争の常道である。また、兵員や武器や弾薬庫が集積されている基地等を先制攻撃して、敵の戦力を弱体化するのも常道であるが、ロシア軍はこれを実現できなかった。

ウクライナは米国からロシア軍の作戦計画全般を知らされており、更に開戦後は、米国がロシアのミサイル攻撃や爆撃攻撃の標的と攻撃時刻とを探知してウクライナ側に通報したので、ウクライナは地対空ミサイルや対空レーダーなどの防空システムや戦闘機を分散、移動、隠匿し、空軍基地にはモックアップを設置するなどしたため、その損害を抑制してロシアの航空優勢確立を阻止できたという<sup>73</sup>。

また、ウクライナ陸軍は、全面侵攻の可能性に備えて、兵員や武器装備、弾薬、燃料、食糧、指揮所など兵力を事前に移動分散し、兵力温存を図っていた。ロシア軍は既知の軍事施設や基地を先制攻撃したが、多くの兵力は既に移動しており、そのためウクライナ陸軍の損害も軽微であった<sup>74</sup>。

### ウ ミサイル巡洋艦モスクワ撃沈（2022年4月14日）

ウクライナ軍は、ロシア黒海艦隊の旗艦ミサイル巡洋艦モスクワをネプチューン対艦ミサイル 2 発とトルコ製無人攻撃機バイラクトルで攻撃し、火災を発生させ旗艦の沈没という戦

<sup>69</sup> Ken Dilanian, et.al., “U.S. intel helped Ukraine ...” ウクライナ空軍による爆撃も行われた。

<sup>70</sup> ヘリボン空挺部隊の撃墜の様子は、CNN でも放送されていた。

<sup>71</sup> Paul Sonne, et.al., “Battle for Kyiv: Ukrainian valor, Russian blunders combined to save the capital,” *The Washington Post*, 24 August 2022, accessed 25 August 2022, [https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/?itid=hp\\_temp3-ukraine](https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/?itid=hp_temp3-ukraine)

ウクライナ軍は、ロシアの侵攻作戦は東部が主体であって全面侵攻の可能性は低いと評価していた。そのために、ホストーメリ空港防衛担当の精鋭部隊は東部方面に移動していたが、その代わりに、万々に備え、同空港の占拠部隊を攻撃する砲兵部隊や対地攻撃機を準備していたのである。

<sup>72</sup> Shane Harris, et.al., “Road to war: U.S. struggled to convince allies, and Zelensky, of risk of invasion.”

<sup>73</sup> Ken Dilanian, et.al., “U.S. intel helped Ukraine ...”

<sup>74</sup> Paul Sonne, et.al., *ibid.*

果を上げた。

米国はウクライナと定期的に黒海のロシア艦船について情報を共有している<sup>75</sup>。この事例では、ウクライナ軍が黒海オデーサ南方を航行中の艦船を発見、米国は確認を求められて艦名モスクワと位置情報を回答したという。ウクライナ軍はその後ネプチューン対艦ミサイルなどで同艦を攻撃した。攻撃の主体はウクライナ軍であるが、同艦の識別と位置情報がなければウクライナ軍は高価なミサイルを使用して攻撃はしなかったであろうから、これもインテリジェンス支援の成果である<sup>76</sup>。

## エ ロシア軍将官 12 人の殺害（2022 年 5 月上旬まで）

2022 年 5 月上旬の段階で、ウクライナ軍はロシア軍の将官 12 人を殺害したとしている。将官殺害 12 人というのは異常に多い数であるが、これはロシア軍の指揮系統に混乱を生み出すものであり、それ自体が大きな戦果である<sup>77</sup>。更に将官が殺害されればその後任補充の必要があり、開戦当初の殺害にはロシア軍の進軍を遅らせる効果もあった<sup>78</sup>。

将官殺害の背景にある米国のインテリジェンス支援は、ロシア軍部隊全ての位置情報であるが、これには移動指揮所の位置やその他の詳細情報も含まれるのである。米国防総省の報道官は、ロシア軍将官殺害のための位置情報は提供していないと発言しているが、その言い回しは、ウクライナ軍自体が情報収集能力を持っており、ウクライナ軍は米国提供情報を含め情報を主体的に分析判断して攻撃に使用しているというものである。他方、ロシア軍の移動指揮所の位置情報の提供自体は否定していない<sup>79</sup>。勿論、移動指揮所の正確な位置情報があれば、そこに所在する指揮官は推定できるのであるから、指揮所を標的に攻撃をすれば将官を殺害できる可能性も高まる。言い回しはともあれ、実際、米国のインテリジェンスが将官殺害を支援しているのである<sup>80</sup>。

---

<sup>75</sup> Shane Harris and Dan Lamothe, “Intelligence-sharing with Ukraine designed to prevent wider war.”

<sup>76</sup> Ken Dilanian, Courtney Kube and Carol E. Lee, “U.S. intel helped Ukraine sink Russian flagship Moskva, officials say,” *NBC News*, 6 May 2022, accessed 6 May 2022, <https://www.nbcnews.com/politics/national-security/us-intel-helped-ukraine-sink-russian-ship-27559>

<sup>77</sup> Julian E. Barnes, Helene Cooper and Eric Schmitt, “U.S. Intelligence Is Helping Ukraine Kill Russian Generals, Officials Say,” *The New York Times*, 4 May 2022, accessed 5 May 2022, [https://www.nytimes.com/2022/05/04/us/politics/russia-generals-killed-ukraine.html?campaign\\_id=60&emc=edit\\_na\\_20220504&instance\\_id=0&nl=breaking-news&ref=cta&regi\\_id=189263598&segment\\_id=91315&user\\_id=784c7a7d37c1ab1c05d5af4534d46768](https://www.nytimes.com/2022/05/04/us/politics/russia-generals-killed-ukraine.html?campaign_id=60&emc=edit_na_20220504&instance_id=0&nl=breaking-news&ref=cta&regi_id=189263598&segment_id=91315&user_id=784c7a7d37c1ab1c05d5af4534d46768)

<sup>78</sup> William Booth, Robyn Dixon and David L. Stern, “Russian generals are getting killed at an extraordinary rate,” *The Washington Post*, 26 March 2022, accessed 2 June 2022, <https://www.washingtonpost.com/world/2022/03/26/ukraine-russian-generals-dead/>

<sup>79</sup> Department of Defense, *Press Briefing by Pentagon Press Secretary John F. Kirby*, 5 May 2022, accessed 7 May 2022, <https://www.defense.gov/News/Transcripts/Transcript/Article/3022007/pentagon-press-secretary-john-f-kirby-holds-a-press-briefing/>

<sup>80</sup> なお、正確な位置情報が判明した移動指揮所或いは将官を攻撃する方法としては、ピンポイントでの砲撃、或いは、狙撃専門部隊による狙撃が挙げられる。

## オ ロシア軍渡河作戦の阻止（2022年5月上旬）

2022年5月上旬、ロシア軍は東部ルハンシク州の要衝を攻撃するためにドネツ川の渡河作戦を行ったが、11日渡河作戦中の第74自動車化狙撃旅団は砲撃を受け大損害を被り渡河作戦は失敗した。その損害は、一個大隊戦術集団の兵員装備の壊滅に相当するという<sup>81</sup>。

榴弾砲による砲撃で渡河作戦を阻止して大損害を与えるには、渡河時に榴弾砲を正確に一点に集中砲撃する必要がある。それを実現するには、遠距離に配置された榴弾砲を連携させて砲撃する必要があり、広域射撃管制アプリ GIS Arta とイーロン・マスク提供のスターリンク衛星通信が貢献したと報道されている<sup>82</sup>。更にまた、ロシア軍の動きを事前に把握すること、射撃管制のための正確且つ詳細な三次元（3D）デジタル地図が不可欠となる<sup>83</sup>。

推定であるが、ロシア軍の動向については米国がインテリジェンス支援をしているであろうし、また三次元デジタル地図については、米国イミント機関・国家地理空間諜報庁 NGA が関与している可能性が高い。NGA が正確なデジタルマップを提供したか、或いはマップ作成の技術支援をしたと推定できる<sup>84</sup>。

## カ セヴェロドネツク・リシチャンシク攻防戦（2022年5月～7月上旬）

セヴェロドネツク、リシチャンシク両市では、5月以降ロシア軍との間で激しい攻防戦が行われた。両市は、純軍事的にはそれ程の重要性はないものの、政治的にはルハンシク州内でウクライナ政府支配下の最後の拠点都市であり、両市が占領されれば、ロシア軍がルハンシク州全域を支配することとなる。そこで、ウクライナ軍は防衛のため精鋭4個旅団以上、数万人を配置して戦ったが、6月に入ると両市地域の北東南の三方面はロシア軍に包囲され、西方の脆弱な兵站線を遮断されれば部隊全滅の虞があった。そこで、一部の軍事評論家は、包囲全滅を避けるため早期撤収の必要を指摘していた。しかし、ウクライナ軍は頑強に抵抗を続けた後、漸く7月上旬に部隊を撤収した。

ウクライナ軍が、一見包囲全滅の危険を冒して7月上旬まで2か月も抵抗を続けた背景には、政治的要因に加えて、インテリジェンスの力があると推定する。即ち、セヴェロドネツク、リシチャンシク周辺のロシア軍の戦力（部隊規模、装備、士気その他）を正確に把握していたために、包囲全滅のリスクを避けつつ、戦闘を継続できたのではないか。そしてその背景には、ウクライナ自らのインテリジェンス力に加えて米国からのインテリジェンス支援があったと見られる。

## キ HIMARS（高機動ロケット砲システム）の効果的運用（2022年6月下旬以降）

ウクライナは、米国から HIMARS を 2022年6月23日に4基受領したのを皮切りに9

---

<sup>81</sup> Anton Troianovski and Marc Santora, “Growing evidence of a military disaster on the Donets pierces a pro-Russian bubble,” *The New York Times*, 15 May 2022, accessed 24 May 2022, <https://www.nytimes.com/2022/05/15/world/europe/pro-russian-war-bloggers-kremlin.html>

<sup>82</sup> 青葉やまと「アメリカ軍より優れる——ウクライナ内製ソフトで砲撃20倍迅速に」『ニューズウィーク』2022年5月26日、閲覧同26日、<https://www.newsweekjapan.jp/stories/world/2022/05/20-107.php>

<sup>83</sup> 「英国防省の分析で判明『ロシア軍は東部戦線で大惨敗』“投入軍3分の1を失う”の重要な意味」『デイリー新潮』2022年5月19日、同日閲覧、<https://www.dailyshincho.jp/article/2022/05191052>

<sup>84</sup> 「3（2）イミント・プラットフォーム」の記述も参照。

月までに合計 16 基受領している（米国防総省は、10 月 28 日には総計 38 基の供与（予定）を表明している<sup>85</sup>）。これは射程 80 キロで精密誘導のできるロケット砲システムであり、従来ウクライナ軍が攻撃できなかったロシア軍の後方施設をピンポイントで攻撃できる兵器である。受領後、弾薬倉庫や指揮所などの攻撃で成果を上げている<sup>86</sup>。2022 年 9 月 8 日のミリ－米統合参謀本部議長の発言によれば、標的 400 個以上を破壊し、ロシア軍の兵站や指揮系統に重大な支障を与えている<sup>87</sup>。

ところで、HIMARS が効果を上げるには、標的である弾薬倉庫、指揮所や装甲車修理所の正確な位置を把握する必要がある。そしてここでも、米国のインテリジェンス支援が効果を発揮している。ウクライナ軍の HIMARS 部隊の砲撃手順は、攻撃したい標的とその位置を特定すると上級司令部に報告する。上級司令部は米軍により正確な位置情報の提供を求め、その情報を得て実際のロケット砲撃を行う。ウクライナ軍の把握した位置情報は不正確な場合もあり、米軍から正確な位置情報が提供されない場合は砲撃しない。貴重なロケット弾を無駄にしたくないからである<sup>88</sup>。

#### ク トルコ製 UAV バイラクタルの効果的運用

今次戦争では無人飛行体 UAV の活躍が注目されているが、特に、ウクライナ軍はトルコ製 UAV バイラクタルをロシア軍に対する偵察と攻撃に効果的に運用している（開戦時 20 機保有）。このバイラクタルの効果的運用にも米国のインテリジェンス支援が貢献している。

元空将補の宮脇俊幸氏によれば<sup>89</sup>、先ず、ロシア侵攻時の損害回避である。バイラクタルの常設基地はウクライナ南部にあったが、侵攻前にウクライナ西部の小規模施設に分散配備

---

<sup>85</sup> DoD, Fact Sheet on U.S. Security Assistance to Ukraine, July 18, 2022, <https://media.defense.gov/2022/Oct/28/2003104896/-1/-1/1/UKRAINE-FACT-SHEET-OCT-28.PDF>. なお、これ以降は 2023 年 7 月に至るまで、HIMARS の供与予定数に変化はない。

<sup>86</sup> Eric Schmitt and John Ismay, “Advanced U.S. Arms Make a Mark in Ukraine War, Officials Say,” *The New York Times*, 1 July 2022, accessed 13 July 2022., <https://www.nytimes.com/2022/07/01/us/politics/himars-weapons-ukraine.html>

<sup>87</sup> DOD, *Secretary of Defense Lloyd J. Austin III and Chairman of the Joint Chiefs of Staff Army General Mark A. Milley Hold a Press Conference Following the Ukraine Defense Contact Group Meeting, Ramstein Air Force Base, Germany*, 8 September 2022, accessed 9 September 2022, <https://www.defense.gov/News/Transcripts/Transcript/Article/3152582/secretary-of-defense-lloyd-j-austin-iii-and-chairman-of-the-joint-chiefs-of-sta/>

<sup>88</sup> Isabelle Khurshudyan, et.al., “Ukraine’s rocket campaign reliant on U.S. precision targeting, officials say,” *The Washington Post*, 9 February 2023, accessed 11 February 2023, <https://www.washingtonpost.com/world/2023/02/09/ukraine-himars-rocket-artillery-russia/>

本記事によれば、ウクライナ側は、米軍からの正確な位置座標情報の提供がなければ砲撃しないのであるから、米軍からの情報提供無しでのロシア領攻撃はありえないと主張して、より長射程のロケット弾やミサイルの提供を要請している。（2023 年 2 月現在、米国の提供するロケット弾の射程は 50 マイルである。）

また、米軍の問合せ窓口は NATO 域内の米軍施設であるが、安全のため基地名は報道しないとされている。他の情報から判断して、米欧州軍司令部 EUCOM のインテリジェンス部門が所在するドイツ国内の基地であろう。

<sup>89</sup> 宮脇俊幸「ウクライナ軍無人機、善戦の理由」『軍事研究』第 57 巻第 8 号（2022 年 8 月 1 日）、42－55 頁。

した。当然、米国の情報に基づく措置である。

次に、運用時にはロシア軍の地対空ミサイルに撃墜されないようにする必要があるが、ロシア軍の中・短距離ミサイル「ブーク」等に対しては、その隙をついて破壊した。つまり、ミサイルの陣地転換、整備などのためレーダを停止する隙をウクライナ軍は地上や空中から探知して、バイラクトルによって攻撃したと推定している<sup>90</sup>。その前提としては、当然に中・短距離ミサイルの位置情報が必要で、米国のインテリジェンス支援があったと見られる。また、ロシア軍の長距離地対空ミサイル S300、S400 はバイラクトルによる攻撃は難しいので、米国のインテリジェンス支援により S300、S400 の位置情報を得て、そのレーダに捕捉されない様に低高度で飛行するなどの運用をしていると推定している。

何れにしろ、バイラクトルの効果的運用の背後にも米国によるインテリジェンス支援の存在が推定される。

#### ケ ハルキウ州の奪還作戦（2022年9月7日～10月中旬）

ウクライナ軍は、9月7日突然ハルキウ州全域の奪還のための攻勢作戦を開始し、ロシア軍の防衛線を突破して7日、8日の2日間で50キロも突出し、約1週間でオスキル川までのハルキウ州の大部分を奪回した。他方、虚を突かれたロシア軍は混乱して壊走し、多くの武器弾薬を放置して退却した。

この作戦が成功した要因は、ロシア軍精鋭部隊がヘルソン州やドンバス地方の戦闘支援のためにハルキウ州から転出して、ロシア軍兵力が手薄になっていたためである。しかし、兵力が手薄になった事実とハルキウ州に残存するロシア軍部隊の展開状況について正確且つ詳細な情報がなければ、今回の攻勢のような作戦は不可能である。

攻勢作戦の背景には、ウクライナ自体による情報収集もあったであろうが、当然、米国によるインテリジェンス支援の貢献もあったであろう。今回の作戦に関しては、米軍関係者と相当の情報共有がなされていたと報道されている。

以上が判明しているインテリジェンス支援の具体的事例である。これらの多くは匿名の関係者情報として報道されそれに関するホワイトハウスや国防総省の報道官と記者の遣取から判断して間違いないと判断したもの、或いは四圍の状況から間違いがないと判断したものであるが、これら判明事例は全体の極一部である。ウクライナ軍の日々の作戦立案・実行では、米国によるインテリジェンス支援が大きく貢献しているのは間違いない。

### （4）サイバー防衛支援

#### ア 開戦前の支援

2014年ロシアはクリミア半島を占領し、東部ドンバス地方の一部に親露派民兵による支配地域を作り出したが、その際のロシアによるサイバー攻撃にウクライナは殆ど抵抗することが出来なかった。

そこで、ウクライナは米国などに協力を求め、対策を進めてきた。

---

<sup>90</sup> 宮脇氏は、レーダ停止の探知はウクライナ軍によると推定している。筆者は、これも米国の各種エリート収集システムで探知したデータ分析情報を得た可能性があると見る。

米国は2014年以降、ウクライナのサイバー対策に支援を行い、技術訓練などを施してきた。更に2018年からは、米サイバー軍が対ロシア作戦や訓練のため関係者をウクライナに送り込み、4000万ドル以上の支援を提供してきた<sup>91</sup>。その結果、ロシアのサイバー攻撃の担い手の所在や正体、技術や戦術について広く深い知識を事前に蓄えることができた<sup>92</sup>。

サイバー軍による支援の重要な柱が、**Hunt Forward** 作戦である。これは一言でいえば、ネットワーク中のマルウェアなどの脅威を **hunt** (狩る) する活動、マルウェア狩りである。ウクライナでは2018年以来複数回行われ、直近の派遣は2021年12月と全面侵攻直前の時期であった。HF 作戦は通常、サイバー軍の直轄部隊、サイバー国家任務部隊 (Cyber National Mission Force) から、作戦チームを2~3月間派遣し、調査対象のネットワークに機材を接続してマルウェアの有無やシステムの脆弱性を調査する。同部隊の強みは、第1にNSAサイバーセキュリティ局と緊密に協力し、同局から敵対国のシグント部隊 (ハッカー集団) についての情報を入手できること。第2に民間企業との協力で、民間企業の持つ脅威情報を入手できることである。こうして派遣チームは、(敵対国の) 容疑性の高い特定IPアドレス情報や、マルウェアの特徴指標 (signatures) の情報を持って派遣されるのである。

全面侵攻開始時期のHF作戦は、情勢が緊迫しており、史上最多の約40人が派遣された。そして2022年1月中旬には、ロシアによるサイバー攻撃第一波 (ワイパー攻撃) が始まったため、この攻撃対処の支援にも取り組んだ。数日にしてキーウは占領されると予測されていた時期で、危険を冒して予定を延長して2月末まで残留して活動したのである。派遣チームがウクライナで挙げた成果は、第1に派遣チームが担当した3つのネットワークは、1月中旬のワイパー攻撃の被害を受けなかったことである。また第2に、ウクライナ当局との協力で相当量のマルウェアを入手し、侵入 (compromise) の特徴指標6000以上を共有できたことであるという。これら情報は米国のサイバーセキュリティ対策にも寄与している。緊迫した状況での協力の結果、派遣チームとウクライナ当局との信頼が深まり、その後も円滑な協力関係が継続しているという<sup>93</sup>。

更にウクライナは、米サイバー軍やNSAなどの政府機関に加え、民間のサイバーセキュリティ専門企業や大手IT企業の協力を受け、チームとしてのサイバー防衛を実行できる態勢が構築された。

## イ 米国サイバー軍、NSA 他

米国インテリジェンスは、ウクライナのサイバー防衛を支援している。2022年6月1日に米サイバー軍司令官兼NSA長官ナカソネ大將は、ウクライナ戦争に関して米国は防禦作戦、攻撃作戦、情報作戦の全ての領域で作戦を実施してきたと述べている<sup>94</sup>。当然、具体的

<sup>91</sup> 山田敏弘「サイバー攻撃で『ロシア圧勝』のはずが。。。人類初のハイブリッド戦争はなぜ大失敗した？」(『Newsweek』2022年9月22日) 2022年9月22日閲覧。

<sup>92</sup> Mike Rogers インタビュー「サイバー防衛、究極の団体戦」2022年10月14日付け『日本経済新聞』

<sup>93</sup> 拙著「**Hunt Forward** 作戦とは何か」茂田インテリジェンス研究室、2023年7月30日。

<https://shigetadayoshi.com/2023/07/30/what-is-hunt-forward-operation/>

同「ウクライナにおける **Hunt Forward** 作戦」茂田インテリジェンス研究室、2023年7月30日。

<https://shigetadayoshi.com/2023/07/30/hunt-forward-operation-in-ukraine/>

<sup>94</sup> 2022年6月1日、英国スカイニュースの取材に対して、米サイバー軍司令官 (兼NSA長官) ナ

内容については言及がない。防衛作戦の一部は先に述べた HF 作戦であるが、それは全体の一部にすぎないであろう。全体像については、元米国家諜報長官デニス・ブレア氏の貴重な発言がある。ブレア氏の発言を手掛かりにして、米国によるインテリジェンス支援の内容について述べたい。

デニス・ブレア氏は、ロシアのウクライナに対するサイバー攻撃は軍事攻撃以上に失敗しているとして、その理由に挙げたのが、①ウクライナ側の努力（重要な官民ネットワーク保護システムの導入）、②米国等支援国によるロシアの攻撃の無力化、③米国とウクライナ担当者の協力（共にサイバー情報を収集し防衛に当たっている）の三つを挙げている<sup>95</sup>。

特に注目されるのは、②の米国等支援国によるロシアの攻撃の無力化である。ブレア氏は「米国をはじめウクライナの友好国や支援国は、ウクライナ側のサイバー防御に協力するだけでなく、ロシアの攻撃を直接無力化しています。」と述べている<sup>96</sup>。これは要するに、米国初め UKUSA 諸国が前進防衛（Defend Forward）を通じて、ロシアの攻撃を阻止しているということである。

具体的には、NSA 初め UKUSA 諸国のシグント機関は、サイバー攻撃対策で既に 10 年以上前から「積極防衛」に取り組んできた。これは、事前に（攻撃してくる可能性のある）脅威グループを解明して、攻撃を受ける前に防衛対策を準備しておくものである。対策は当初は、守るべきシステムとインターネットとの結節点に事前に防衛システムを設置することであったが、それでは十分でないとして 2018 年からは「前進防衛」に取り組み始めた。これは脅威グループの攻撃を、インターネット空間、或いは、敵空間（相手方のネットワーク内）において防衛することである。何れにしろ「積極防衛」「前進防衛」のためには、事前に脅威グループのシステムに侵入して脅威を解明する作業が不可欠である<sup>97</sup>。

この点についてブレア氏は「サイバー防衛の重要な要素は、相手のネットワークに侵入し、脅威は何か、如何に攻撃を回避できるかを把握することです。」<sup>98</sup>と述べている。相手のネットワークに侵入するのは、相手方が味方の政府、企業、大学などのネットワークに侵入した場合にその足跡をたどって相手方のコンピューターまで侵入する場合もあるが<sup>99</sup>、攻撃を受ける前に相手方のシステムに侵入して脅威を解明しておくことが望ましいのである。

米国では、前進防衛の実施そのものは基本的にサイバー軍の任務であるが、その前段の脅

---

カソネ大將は、ウクライナ戦争に関して米国は防衛作戦、攻撃作戦、情報作戦の全ての領域で作戦を実施してきたと述べている。

--Alexander Martin, "US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command," *Sky News*, 1 June 2022, accessed 2 June 2022, <https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139>

<sup>95</sup> デニス・ブレア他「日本のサイバー能力は『マイナーリーグ』』『正論』6月号（2022年5月2日）、48頁。

<sup>96</sup> デニス・ブレア他、前掲。

<sup>97</sup> この詳細については、拙著『サイバーセキュリティとシグント機関～NSA 他 UKUSA 諸機関の取組～』（情報セキュリティ総合科学第 11 号、2019 年 11 月）参照。

<sup>98</sup> デニス・ブレア他、50 頁。

<sup>99</sup> デニス・ブレア他、55 頁。

威グループの解明においては、シグント機関 NSA のノウハウとシグント・インフラが不可欠である。NSA 長官とサイバー軍司令官は同一人物であり、両機関が協力して当たっているのである。

ロシア・ウクライナ戦争では、米サイバー軍と NSA、更に UKUSA 同盟諸機関も参加して、ロシアの脅威グループによる攻撃をインターネット空間で阻止し、又は相手のシステムを攻撃して阻止しているのである。ブレア氏は、ロシアのサイバー攻撃は軍事攻撃以上に失敗していると述べており、NSA 初め UKUSA 諸機関による防衛が水面下で大々的且つ効果的に行われていると推定できる。

また、③の米国とウクライナ担当者の協力については、後述するが、ウクライナのセキュリティ・サービス SSU は、4月に NATO のサイバー脅威の情報共有組織に参加したことが公表されている。

## ウ 民間企業

### ① 民間企業によるウクライナ支援

サイバーセキュリティにおけるウクライナ支援で注目されるのは、サイバー空間で大きな影響力を持つ米国系の主要 IT 企業が、米国政府の勧奨を受けて、協調してサイバー防衛支援に貢献していることである。

これには米国の元政府高官のグレッグ・ラットレイ博士が関与している。彼は元米空軍のシグント将校であり、米国家安全保障会議のサイバーセキュリティ責任者を経験した専門家である。ラットレイ博士は、全面侵攻前からウクライナ政府にサイバーセキュリティについて助言をしてきたが、全面侵攻後は、ウクライナに対する民間企業による支援協力組織「サイバー防衛支援共同体」(Cyber Defense Assistance Collaborative) の指導者として、米国政府指導者やサイバー関係組織への助言、米国によるサイバー支援の助言に従事してきたという。つまり、現在は形式的には民間人であるが、元政府高官の専門家が、民間企業によるウクライナ支援の調整に従事しているのである。博士によれば、米国を始めとする西側の IT 企業は協力してウクライナに対するサイバー攻撃を監視し対応策をとっているという<sup>100</sup>。

例えば、ロシアは全面侵攻直前に 48 の省庁や企業のシステムに対してデータ破壊目的のサイバー攻撃を仕掛けたが、マイクロソフト社はこれらの攻撃を AI を使って探知し警告を発するなど、直接的なサイバー防衛でも貢献している<sup>101</sup>。アルファベット社 (グーグル) も、ロシアのハッカー集団についての情報をウクライナ政府に提供するなどしてウクライナのサイバー防衛に貢献している<sup>102</sup>。

<sup>100</sup> Greg Rattray, "US-Japan Cyber Cooperation and Lessons Learned from Ukraine," (「ソリトン エグゼクティブフォーラム 2022」講演。東京、2022年10月25日)

<sup>101</sup> Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*, pp.5-9, 22 June 2022, accessed 28 August 2022, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK>

<sup>102</sup> Vivian Alama and Dustin Volz, "State Department Urges Silicon Valley to Aid National Security Effort," *The Wall Street Journal*, 15 October 2022, accessed 18 October 2022, <https://www.wsj.com/articles/state-department-urges-silicon-valley-to-aid-national-security-effort-11665835204?mod=djemCybersecurityPro&tpl=cy>



特に注目されるのが、マイクロソフト社である。同社は、全面侵攻前の 2021 年 10 月からエンジニアをウクライナに派遣するなどしてサイバー防衛を全面的に支援している<sup>103</sup>。マイクロソフト社は米国政府 NSA に協力的なことで知られており、全面支援も裏で NSA の勸奨があったものと推定できる。具体的には例えば、ウクライナでは政府データの保管は全て政府のデータセンターなど政府施設内に限定していたが、戦争となればこれら施設が物理的攻撃やサイバー攻撃を受けるのは明白であった。そこでウクライナ政府は全面侵攻直前の 2022 年 2 月 17 日に方針を変更し、データ保管をクラウド化して欧州諸国のデータセンターに分散保管することを可能とした。マイクロソフト社はこれを受けて、ウクライナの 20 省と 100 以上の政府機関・政府系企業のデータのクラウド化を行い、ウクライナの政府機能の維持に貢献している<sup>104</sup>。実際の経緯は、サイバー防衛に関して、マイクロソフト社を含む米国・ウクライナ政府関係者による事前協議が行われて、ウクライナ政府データのクラウド化の方針が決定され、それに従いウクライナ政府が法令改正を決定し、マイクロソフト社による作業が開始されたのであろう。

また、アマゾン社（アマゾン・ウェブ・サービス）もウクライナ政府のデータのクラウド化に協力している<sup>105</sup>。アマゾン社は、住民登録、土地登記簿、納税履歴などのデータを同社のクラウドコンピューティングに移行させた。作業は、全面侵攻開始の 2 月 24 日後に開始され、サーバー 3600 台のデータを 45 日以内にクラウド化したという<sup>106</sup>。

ラットレイ博士によれば、ウクライナのサイバーセキュリティ対策において、データのクラウド化は大きな効果を生んでいる<sup>107</sup>。また、米サイバー軍のハートマン少将も同様の見解を述べている<sup>108</sup>。

他にイーロン・マスク氏はスターリンク衛星通信のサービスをウクライナに提供しており、ロシアによるウクライナの衛星通信の妨害に対抗している<sup>109</sup>。更に、データ解析会社の

---

<sup>103</sup> Microsoft, *ibid.*

—山田敏弘「ウクライナ侵攻の裏にある『見えない戦争』とサイバー工作」（『時事通信』2022 年 4 月 21 日）、閲覧 6 月 19 日。

[https://www.jiji.com/jc/v8?id=202204ukrrusyt&utm\\_source=yahoo&utm\\_medium=referral&utm\\_campaign=link\\_back\\_auto\\_custom+](https://www.jiji.com/jc/v8?id=202204ukrrusyt&utm_source=yahoo&utm_medium=referral&utm_campaign=link_back_auto_custom+)

—藤井彰夫「デジタルと戦争と改革と」（『日本経済新聞』2022 年 7 月 4 日）

—山田敏弘「サイバー攻撃で『ロシア圧勝』のはずが。。人類初のハイブリッド戦争はなぜ大失敗した？」前掲。

<sup>104</sup> Microsoft, *ibid.*

<sup>105</sup> Barry Hatton, “Microsoft extends aid for Ukraine’s wartime tech innovation,” *The AP News*, 3 November 2022, accessed 4 November 2022, <https://apnews.com/article/kyiv-technology-portugal-lisbon-brad-smith-2336193477680e6822dbde3f50250385>

<sup>106</sup> 「アマゾン支援の舞台裏～ウクライナから重要データ『避難』」『日本経済新聞』2022 年 12 月 4 日。アマゾン社幹部のリアム・マックスウェル氏の取材記事である。

<sup>107</sup> Greg Rattray 前掲。

<sup>108</sup> Dina Temple-Raston, “Exclusive: Inside an American hunt forward operation in Ukraine,” *The World*, 30 June 2023, last accessed 30 July 2023, <https://theworld.org/stories/2023-06-30/exclusive-inside-american-hunt-forward-operation-ukraine>

<sup>109</sup> イーロン・マスク氏は開戦直後に要請を受け、SpaceX スターリンクの可搬型通信局 1 万台以上

パランティア社もウクライナ軍の戦争努力を全面支援している。このような米国系 IT 企業の支援の背景には、米国政府による水面下の支援が推定される。

## ② 背景：米国における官民連携

このような米国系 IT 企業によるウクライナ支援の背景には、米国自体における官民連携の進展が挙げられる。NSA は 2020 年 12 月にサイバーセキュリティにおける官民連携の窓口として、Cybersecurity Collaboration Center（サイバーセキュリティ協働センター）を開設した。同センターの任務は、NSA がシギント活動によって得た機密の知見を基礎に民間企業を持つ脅威情報と専門技術を総合して、脅威に対抗するために有効な情報を民間企業に迅速に提供することとしている。センター加盟企業名は非公表であるが、クラウドコンピューティングや通信企業、サイバーセキュリティ企業、防衛産業などが参加し、発足 1 年後には 100 社以上が参加し、**2023 年 6 月現在では参加企業は約 500 社にも上っている**<sup>110</sup>。マ

---

と通信サービスを提供した。その後通信局は 1 万 5 千台に増加。内数千台は無償提供。他に、米国政府と民間企業がそれぞれ数千台の費用を負担している。スターリンク通信システムは、今やウクライナ軍の指揮通信の基幹をなしているだけでなく、兵士への一般情報連絡、家族との通信、戦闘地域住民との連絡、更には通信会社ウクルテレコムシステムの保守管理など幅広く使用されている。スターリンク無しでは戦闘継続はできなかつたとまで言われるほど、ウクライナの通信機能の確保に大きな貢献をしている。Yaroslav Trofimov, Micah Maidenberg and Drew FitzGerald, “Ukraine Leans on Elon Musk’s Starlink in Fight Against Russia,” *The Wall Street Journal*, 16 July 2022, accessed 18 July 2022, <https://www.wsj.com/articles/ukraine-leans-on-elon-musks-starlink-in-fight-against-russia-11657963804>

また下記の NHK World 番組で、特殊通信・情報保護庁長官は、ロシア軍全面侵攻前に通信システムに対する攻撃予測を知らされていたと述べ、代替通信システムとしてのスターリンクの重要性に言及している。通信システム攻撃の予測とイーロン・マスク氏のスターリンク通信提供の手際の良さに鑑みると、スターリンク通信のサービス提供は、全面侵攻前から米国政府機関も関与して調整が進んでいた可能性がある。“Ukraine: The New Satellite War – Digital Eye,” *NHK World*.

2022 年 10 月 19 日現在、ウクライナにはスターリンク端末が約 2 万 5 千台あり、病院から銀行まで市民生活や生命線とされる社会機能の維持を支えてきた。また、ウクライナ軍も作戦に活用。ジリアン・テット 『通信依存』マスク氏で露呈』2022 年 10 月 19 日付『日本経済新聞』Financial Times 記事転載。

2023 年 6 月 1 日、国防総省は、SpaceX スターリンクの通信使用料を国防総省が負担する合意が成立したと発表した。イーロン・マスク氏は、2022 年 10 月にウクライナのための費用負担額が月 2000 万ドルに近づいていると苦情を述べていたが、国防総省の負担額は開示されていない。Micah Maidenberg and Matthew Luxmoore, “Pentagon Agrees to Pay SpaceX For Satellite Internet in Ukraine,” *The Wall Street Journal*, 1 June 2023, last accessed 27 July 2023, <https://www.wsj.com/articles/pentagon-agrees-to-pay-spacex-for-satellite-internet-in-ukraine-2bdf3bf4>

<sup>110</sup> NSA Cybersecurity Collaboration Center, <https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Overview/>

--Joseph Marks, “NSA is surging its collaboration with the private sector,” *The Washington Post*, 21 October 2021, accessed 4 November 2022, <https://www.washingtonpost.com/politics/2021/10/21/nsa-is-surging-its-collaboration-with-private-sector/>

-- NSA, *NSA’s Cybersecurity Collaboration Center Celebrates its First Year*, 22 December 2021, accessed 4 November 2022, <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2881886/nsas-cybersecurity-collaboration-center-celebrates-its-first-year/>

マイクロソフトやグーグルなど米国の主要 IT 企業は当然参加しているであろう。

次に 2021 年 8 月に、CISA (Cybersecurity and Infrastructure Security Agency) <sup>111</sup>も官民連携の枠組 Joint Cyber Defense Collaborative (サイバー防衛共同体) を作った。主目的は、米国全体のサイバー防衛計画の策定であり、被害を未然に防止するための官民協力の枠組みである。参加官庁は、国防総省、サイバー軍、NSA、司法省、FBI、DNI 室であり、民間企業では、Amazon Web Services、AT&T、CrowdStrike、FireEye、Mandiant、Google Cloud、Lumen、Palo Alto Networks、Verizon などの企業が参加している<sup>112</sup>。

このような民間企業との協力関係を背景に、米国政府は 2021 年後半に、民間企業に対してロシアによるウクライナ侵攻の可能性についてブリーフィングを行い、次に、米国政府は複数のサイバーセキュリティ企業と協力し米国の防禦力を高めると共に同盟国との知見を共有し、サイバー攻撃に備えていったという<sup>113</sup>。

このような米国における官民連携の進展が、2021 年後半以降、米国系 IT 企業によるウクライナ支援の進展の背景をなしているのである。

#### (5) 補足：ウクライナ支援と Give & Take の原則

ところで、米国はウクライナに対するインテリジェンス支援で十分なインテリジェンスの対価を得ているのだろうか。

そもそもインテリジェンスの協力とは、基本的に Give & Take の関係であり、通常一方的

---

-- DHS, "HSToday Q&A: Inside the NSA Cybersecurity Collaboration Center's Mission and Goals with Chief Morgan Adamski," *Homeland Security Today*, 17 October 2022, accessed 4 November 2022, <https://www.hstoday.us/featured/hstoday-qa-inside-the-nsa-cybersecurity-collaboration-centers-mission-and-goals-with-chief-morgan-adamski/>

- Martin Matishak, "Cyber Command to expand 'canary in the coal mine' unit working with private sector," *The Record*, 28 June 2023, last accessed 30 July 2023, <https://therecord.media/cyber-command-under-advisement-team-cyberthreat-collaboration>

<sup>111</sup> 2021 年 7 月に長官に就任したジェン・イースタリー女史の前職は NSA 高官であり、バイデン政権で新設された国家サイバー長官に就任したクリス・イングリシ氏の前職は NSA 副長官である。これらの人事は、米国のサイバーセキュリティにおける NSA の重要性を反映している。

<sup>112</sup> Frank Konkell, "CISA Stands Up Joint Cyber Defense Collaborative," *Nextgov*, 5 August 2021, accessed 13 August 2021, <https://www.nextgov.com/cybersecurity/2021/08/cisa-stands-joint-cyber-defense-collaborative/184322/>

—Chris Riotta, "CISA launches joint cyber defense effort," *GCN*, 6 August 2021, accessed 13 August 2021, <https://gcn.com/cybersecurity/2021/08/cisa-launches-joint-cyber-defense-effort/316202/>

—CISA, *JOINT CYBER DEFENSE COLLABORATIVE*, <https://www.cisa.gov/jcdc>

--Douglas Clark, "CISA launches new joint cyber defense collaborative," 5 August 2021, updated 6 August 2021, <https://homelandprepnews.com/stories/72171-cisa-launches-joint-cyber-defense-collaborative/>

<sup>113</sup> 松原美穂子「サイバー防衛『情報共有』の教訓」(『産経新聞』2022 年 11 月 7 日付)

に無償で情報を提供することはない。インテリジェンスの協力とは博愛事業ではないからである。この点は、シグント情報に関するスノーデン漏洩情報に明確に記述されている。即ち、インテリジェンスの協力は、それがそれぞれの国家諜報要求の充足に貢献する場合、即ち Give & Take の関係が成立する場合に行われる<sup>114</sup>。

しかし、この原則には例外がある。スノーデン漏洩資料でも、危機的状況に於いては一方的なインテリジェンス支援があり得るとしている。つまり、危機的状況にある国を支援することに米国の国益が合致する場合には、インテリジェンス面だけを見れば Give & Take は成り立たなくても、国益全体の立場から支援をすることがあり得るということである。正に、現在のウクライナ戦争におけるインテリジェンス支援である。ウクライナという民主主義国家をロシアという専制国家の侵略から守ること自体が、米国の国益に合致する。従って、インテリジェンス面だけを見れば Give & Take は成り立たないが、総合的な国益の観点からインテリジェンス支援をしているのである。

## 6 ウクライナ SSU によるインテリジェンス

ウクライナには極めて高い能力を持つセキュリティ・サービス SSU (Security Service of Ukraine) が存在し、これがウクライナの戦争遂行に大きく貢献している。戦争遂行では、軍諜報機関や対外諜報機関の重要性は言うまでもないが、セキュリティ・サービスというインテリジェンス機関も重要な役割を担っている。そこで、ウクライナの SSU が果たしている役割について、同機関のウェブサイトなどを参考に記述する<sup>115</sup>。

### (1) ウクライナ・セキュリティ・サービス SSU<sup>116</sup>

セキュリティ・サービス SSU (職員数平時約 2 万 7 千。非常時 3 万 1 千) は、ウクライナ最大のインテリジェンス機関である。防諜、国家体制擁護、テロ対策、サイバーセキュリティ対策、国家機密保持を主任務としており、アルファという特殊作戦部隊を保持している。

元々、ソ連 KGB ウクライナ支局であったが、1991 年ウクライナ独立に伴い、ウクライナの政府機関となった。ソ連 KGB がそうであったように広汎な業務を管轄していたが、独立後、国境警備隊、警護部、対外諜報部、特殊通信・情報保護部などが分離された<sup>117</sup>。

---

<sup>114</sup> スノーデン漏洩資料、NSA, Foreign Affairs Directorate, *What Are We After with Our Third Party Relationship? – And What Do They Want from Us, Generally Speaking?* 15 September 2009, accessed 4 December 2014, <https://firstlook.org/theintercept/document/2014/03/13/third-party-relationships/?Edi>

<sup>115</sup> SSU のウェブサイト自体が、ウクライナによる情報作戦の手段でもあるので、同ウェブサイトに掲示される情報の読み方には注意をする必要がある。

<sup>116</sup> SSU, website, accessed 24 June 2022, <https://ssu.gov.ua/en>

<sup>117</sup> 特殊通信・情報保護部は、遅れて 2005 年に分離されて大統領直属の庁となった。同庁のウエ

SSUは、元はKGBウクライナ支局であったこともあり、当初は親露派が多数を占めていたが、2014年親露派政権の崩壊に伴いSSU長官初め親露派幹部多数がロシアに亡命した。それでも多くの親露派職員が残存しており、全職員に対する尋問とポリグラフ検査を反復することによって、同年末までに親露派職員200人以上を排除した<sup>118</sup>。しかし、これで親露派の排除が完了できた訳ではなく、親露派職員・ロシア協力者の排除はこの後も継続して行われてきた。CIAはCIA職員をSSU顧問として派遣するなどして、このロシア協力者の排除を支援してきた<sup>119</sup>。

## (2) 広汎な通信傍受能力と作戦支援

### ア ウクライナ国内及び周辺における傍受能力

ロシア軍は、2021年に作戦用の暗号通信システムERAを導入したが、部品不足で必要量が生産されていないのか、今次戦争ではこれが十分機能していないようである。そのため、民生用のHF・VHF無線通信や携帯電話を作戦で使用している。更に通信規律が甘く、兵士が勝手に携帯電話で故郷の家族や友人と通信をして軍事情勢について話している。

他方、ウクライナSSUは、広汎な通信傍受能力を持っており、それが今回の戦争で明らかになった。それというのも、SSUが情報工作のためにウェブサイトで傍受情報の一部、主として兵士の私用電話の内容を公開しているからである。ほんの数例を挙げる。

- ロシアFSB将校2人の電話通信：ヴィタリー・ゲラシモフ少将の戦死（2022年3月7日）を話題として、暗号通信網ERAが機能していない状況をこぼした内容<sup>120</sup>。  
(兵站不備)
- ロシア兵士が妻と携帯電話で通信：負傷して早く帰還して報奨金をもらいたいと話している内容<sup>121</sup>。(厭戦気分)

---

ウェブサイトから判断すると、①データネットワークにおける国家情報資源の保護に関する政策の実施、②政府通信諸システム、秘匿通信国家システム、国家情報の暗号的技術的保護の提供を担当している。ウェブサイトの記述から判断する限り、シギント（通信傍受）任務は付与されていない。State Service of Special Communications & Information Protection – Ukraine, website, accessed 6 June 2022, <https://www.cybersecurityintelligence.com/state-service-of-special-communications-and-information-protection-ukraine-7222.html>

<sup>118</sup> Christopher Miller, “Ukraine’s top intelligence agency deeply infiltrated by Russian spies,” *Mashable*, 30 December 2014, accessed 13 May 2022, <https://mashable.com/archive/russian-vs-ukrainian-spies>.

<sup>119</sup> Ken Dilanian, et.al., “U.S. intel helped Ukraine ...”  
—Greg Miller and Catherine Belton, “Russia’s spies misread Ukraine and misled Kremlin as war loomed,” *The Washington Post*, 19 August 2022, accessed 19 August 2022, <https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/?itid=hp-top-table-main-t-2>

<sup>120</sup> Julian Borger, “Vitaly Gerasimov: second Russian general killed, Ukraine defence ministry claims,” *The Guardian*, 8 March 2022, accessed 4 May 2022, <https://www.theguardian.com/world/2022/mar/08/vitaly-gerasimov-second-russian-general-killed-ukraine-defence-ministry-claims>.

<sup>121</sup> SSU, “Invaders dream of getting wounded to get paid and go home (audio),” *News*, 18 April 2022, accessed 1 June 2022, <https://ssu.gov.ua/en/novyny/zaharbnyky-mriiut-pro-svoie->

○ ロシア兵士とロシア国内の友人とのテキストメッセージ（2022年5月24日と25日）：兵站不備のための食糧不足で、犬を食べているという内容<sup>122</sup>。（兵站不備）

公表された通信傍受の事例から判断しても、ウクライナ SSU は、ロシア軍の無線通信、携帯電話、兵士の使用する携帯電話の通話やテキスト通信を広汎に収集して、且つ分析活用する能力を保持していることが分かる。

広汎な傍受能力（通信回線へのアクセスを含む。）は、旧ソ連 KGB の伝統を引き継いでいるのであろう。但し、通信を大量に傍受しているだけでは有効に活用できる訳ではない。有効情報を検索し抽出するソフトウェアが必要である。報道によれば、ウクライナは AI 音声認識技術に優れた米プライマー社に委託して、音声データのテキスト化及びテキストから関心部分を抽出してもらい、作戦に役立てているという<sup>123</sup>。或いは、必要な情報の検索抽出ソフトウェアを米国 NSA から提供されている可能性もある。

公表された通信傍受例の背後には、非公表の通信傍受が大量に存在する。ロシア軍は、作戦に関する通信も非暗号通信が多く、ウクライナは対面するロシア軍の動向に関して重要な情報を収集して、作戦に役立てているのは間違いない<sup>124</sup>。既述したロシア軍将官 12 人の殺害においても、ロシア軍の非暗号化無線通信を傍受して、それ利用して標的（将軍）の詳細位置を特定しているとされる<sup>125</sup>。

#### イ SSU による作戦支援の実例

SSU による通信傍受がどのように作戦支援に活かされているのか、CNN による 2023 年 6 月のルポルタージュ報道<sup>126</sup>があるので紹介しよう。

それは、ウクライナのあるドローン部隊によるロシア軍攻撃の同行取材である。ドローン部隊が夜間ロシア軍ロケット砲陣地の数キロの地点まで密かに接近して、ドローンを離陸させ上空から 16 キロの爆弾を投下する作戦である。ロシア軍に気付かれずに接近し、ドローンを発進させ、目標まで飛行して爆弾を投下した後、迅速にドローンを回収して撤収する。作戦中にロシア軍に探知されれば砲撃を受ける。この作戦中、SSU は関係するロシア軍の

---

poranennia-shchob-otrymaty-vyplaty-ta-poikhaty-dodomu-audio

<sup>122</sup> SSU, “Due to problems with logistics, russian occupiers eat dogs again,” *News*, 31 May 2022, accessed 1 June 2022, <https://ssu.gov.ua/en/novyny/cherez-problemy-z-zabezpechenniam-rosiiski-okupanty-znovu-pochaly-yisty-sobak>

<sup>123</sup> 押切智義、千住貞保「欧米などの民生技術 ウクライナの『武器』に」（『日本経済新聞』2022年5月30日）

<sup>124</sup> 「ロシア軍の無線通信が傍受され軍事報告が筒抜けに、ロシア軍兵士の肉声も公開される」*Gigazine*, 2022年3月26日、閲覧同年5月31日、<https://gigazine.net/news/20220326-russian-forces-radio-transmissions/>

<sup>125</sup> William Mauldin, Thomas Grove and Bojan Pancevsk, “Four Russian Generals Killed in Three Weeks Show Moscow’s Vulnerabilities in Ukraine,” *The Wall Street Journal*, 16 March 2022, accessed 19 April 2022, <https://www.wsj.com/articles/death-of-russian-generals-in-ukraine-expose-vulnerabilities-in-moscows-military-tactics-11647441273>

--William Booth, Robyn Dixon and David L. Stern, “Russian generals are getting killed at an extraordinary rate.”

<sup>126</sup> Vasco Cotovio, et. al., “‘From Ukraine with love:’ The elite night-time drone units bombing Russian military,” *CNN*, 16 June 2023, last accessed 27 July 2023, <https://westobserver.com/news/europe/from-ukraine-with-love-russian-militarys-elite-night-drone-units-bombing/>

通信を傍受して作戦を支援している。本事例では、ドローンがロシア軍陣地に接近すると、ロシア軍兵士は飛行音でドローンを発見、携帯電話のテキストメッセージ機能を使って「鳥が飛んでいる」と隠語で発見報告をしたが、SSUはこのテキストを傍受してドローンが発見されたことを警告。ドローン部隊は、それを受けて、迅速に爆弾を投下して迅速にドローンを回収して、無事撤収した。この事例のようにSSUは通信傍受によって作戦を支援しているのである。

#### ウ 国外に対するコンピューター網工作（CNE）能力

以上で述べた傍受能力の対象は、通信当事者の少なくとも一方がウクライナ国内に居る場合或は無線通信の場合であるが、次のSSUの公表事例を見るとロシア国内の通信と見られるものがある。

- ロシア本国FSB第5総局の内部文書を公表。ロシア国内の世論対策に関するもので、ウクライナに対する「特別作戦」の意義が正しく理解されていないと分析した文書<sup>127</sup>。
- ロシアの守護者プーチンを賛美する際のガイドラインを暴露。ロシア政府職員、芸術家やスポーツ選手が従うべき指針で、秘匿通信回線で政府内に配信されたものを傍受したとしている<sup>128</sup>。

また、SSUのサイバーセキュリティ部長は、対露サイバー攻撃を実施していることを明言している<sup>129</sup>。規模は不明であるがロシア国内に対するコンピューター網工作（CNE、即ちハッキング）も実施しているのは明白であろう<sup>130</sup>。

### （3）国民からの情報収集の組織化

SSUは、広汎な通信傍受能力を持つだけでなく、国民からの情報収集も組織化している。

ウォール・ストリート・ジャーナル紙の現地取材<sup>131</sup>によれば、全面侵攻直後に首都キーウ

---

<sup>127</sup> SSU, “SSU gains access to propaganda manuals of russian special services on ‘correct coverage of special operation’ in Ukraine (video),” *News*, 5 June 2022, accessed 6 June 2022, <https://ssu.gov.ua/en/novyny/sbu-otrymala-dostup-do-propahandytskykh-metodychok-rosiiskykh-spetsluzhb-pro-pravylne-vysvitlennia-spetsoperatsii-v-ukraini-video>.

<sup>128</sup> SSU, “SSU intercepts another FSB manual: they teach russian officials to correctly praise putin and comment on war in Ukraine (video),” *News*, 26 June 2022, accessed 28 June 2022, <https://ssu.gov.ua/en/novyny/sbu-perekhopyla-novi-metodychky-fsb-u-nykh-rosiiskykh-chynovnykiv-vchat-pravylno-khvalyty-putina-ta-komentuvaty-viinu-v-ukraini-video>

<sup>129</sup> SSU, “SSU neutralized hundreds of cyberattacks on Ukrainian cogeneration plants and energy companies in 2022-Illia Vitiuk”, *Mews*, 27 December 2022, accessed 3 January 2023, <https://ssu.gov.ua/en/novyny/z-pochatku-roku-sbu-neitralizuvala-sotni-kiberatak-na-ukrainski-tets-ta-oblenerho-illia-vitiuk>

<sup>130</sup> ウクライナはシグント専門の対外諜報機関は保持していないようである。山田敏弘「ウクライナ侵攻の裏にある『見えない戦争』とサイバー工作」。

<sup>131</sup> Thomas Grove, “How Ukrainian Civilians Risked Their Lives to Help Win the Battle for Kyiv,” *The Wall Street Journal*, 8 May 2022, accessed 8 May 2022, <https://www.wsj.com/articles/how-ukrainian-civilians-risked-their-lives-to-help-win-the-battle->

の郊外ではロシア軍の動向について住民からの情報収集を組織化して首都防衛戦闘に活用した。即ち、キーウ東方の7号線（スーミ・プロバルイ間）は、全面侵攻当初ロシア軍の東からの首都攻略部隊の主たる兵站線であり、兵員や物資の輸送路となっていた。その沿道、キーウ東方約100キロの村人によれば、ロシア軍の侵攻を受け、当初はロシア軍の動向、歩兵砲兵戦車の位置を警察に通報していた。やがて、デジタル変革省がテレグラム通信アプリにチャットボックスを設置し、ロシア軍の動向情報を受信する一元的データベースを構築し、その内容はセキュリティ・サービスSSUと自動的に共有されるようになった。更に、キーウ周辺では既存の行政用デジタル地図アプリ<sup>132</sup>を改修して、グーグル地図上に兵員装備の量と位置情報をピン止め入力してSSUに送信できるようになった。

その成果の一例は、2022年3月上旬キーウ東郊のプロバルイのおける、ロシア軍第90機甲師団2個連隊の戦車梯団の待伏せ攻撃に現れている。先ず梯団先頭を対戦車兵器で同時に後尾を砲撃で撃破し、動けない状態にして大損害を与えたが、砲撃には住民情報が決定的に重要であったという。

このような、ロシア軍の動向についてウクライナ住民からの情報収集は広汎に行われていると考えられる。

ロシア軍占領地では、住民のスマホを取り上げて点検しているとか、住民を地下室に押し込めて出られなくしているとか、更には一部住民の拷問が行われていると報道されているが、ロシア軍からすれば軍の機密保持のため理由のないことではないのである。

#### （４）ロシア工作員・協力者の摘発

##### ア 概要

戦時においては、情報収集や破壊活動のために、工作員を潜入させ或は協力者を運用しようとするのは常套手段である。ロシアは、侵攻に先立って、ウクライナの軍、セキュリティ・サービス、警察機関、検察機関を含む多方面に工作員・協力者を布石してきた。ゼレンスキー政権崩壊後に樹立予定の傀儡政権の首班候補も2人以上準備していたとされる<sup>133</sup>。これに対して、敵国の工作員や協力者を摘発して戦争努力を保護するのは、セキュリティ・サービスの重要な任務である。

ウクライナSSUの発表によれば、2022年2月の全面侵攻から同年5月31日までに、ロシアの工作員360人以上、協力者5000人以上を摘発している<sup>134</sup>。また、同年6月8日現在

---

for-kyiv-11652002200?mod=panda\_wsj\_custom\_topic\_alert

<sup>132</sup> ウクライナにはDiiaという政府公認アプリがあり、これにロシア軍目撃情報の提供機能を搭載しているという報道もある。「【独自解説】ウクライナのIT戦略は最年少大臣が指揮！戦時下でも行政手続き可能なアプリ『Diia』でロシア軍の情報を収集 驚きの“電子戦”を徹底解説」（『ヤフー・ニュース』2022年4月25日配信）、6月6日閲覧、

[https://news.yahoo.co.jp/articles/388c05c167fa113b156924ae54d4be44e03fcaed?](https://news.yahoo.co.jp/articles/388c05c167fa113b156924ae54d4be44e03fcaed?mod=page_1)

<sup>133</sup> “How Russia Spread a Secret Web of Agents Across Ukraine,” *Reuters*, 30 July 2022, accessed 1 August 2022, <https://www.voanews.com/a/how-russia-spread-a-secret-web-of-agents-across-ukraine/6677718.html>

<sup>134</sup> SSU, “SSU exposes russian agent at Ukroboronprom and detains collaborators who gathered intelligence on Ukrainian positions (video),” *News*, 31 May 2022, accessed 1 June 2022,



では破壊活動や情報収集のためのグループ 160 グループ以上を摘発している<sup>135</sup>。

なお、全面侵攻後の 2022 年 3 月 10 日、戒厳令によって、国家反逆罪及び破壊活動の罰則が強化され、終身刑或いは 15 年未満の拘禁刑となった<sup>136</sup>。また、同年 3 月 14 日 SSU は、ロシア軍への協力は国家反逆罪に該当すると警告を発している<sup>137</sup>。

国家反逆罪での検挙事例を見ると<sup>138</sup>、ウクライナ軍部隊や装備の詳細や位置・動向など、戦闘に必要な情報、標的情報や（ロシア軍の）攻撃効果測定情報が多くを占めるが、SSU 将校に関する情報や高速道路上の検問所の位置など、防諜に係わる情報関連の事例もある。更に、後方治安攪乱のためのテロ・破壊活動の未然防止事例もある<sup>139</sup>。

被検挙者は、大きく、全面侵攻直前に浸透した工作員・協力者、思想的な親露派協力者、金目当ての協力者と三つに分類されるが、金目当ての協力者が多いという。検挙現場を同行取材した CNN 報道によれば、SSU は通信傍受によって容疑者を特定し、四捜査によって証拠を固めて検挙に至る事例が多い。2022 年 5 月中旬の検挙事例では、協力者はテレグラム通信アプリを通じて雇われて、報酬は標的情報（部隊の写真と位置情報）1 件約 500 フリヴニャ（約 17 ドル）であった。SSU は数日の調査で検挙し、検挙現場で即座にスマホを証拠品として確保している<sup>140</sup>。また、対露協力者としての被検挙者には、ソーシャル・メディアにロシア支持のメッセージを掲載しただけの者も含まれている<sup>141</sup>。

## イ 特徴的な検挙事例の紹介

典型的なスパイ団の検挙事例、破壊活動の阻止事例、軍や SSU 内部のロシア協力者の検挙事例、大物工作員・協力者の検挙事例、その他特徴的な検挙事例を紹介する。

---

<https://ssu.gov.ua/en/novyny/sbu-vykryla-rosiisku-ahenturu-v-ukroboronpromi-ta-zatrymala-kolaborantiv-yaki-rozviduvaly-pozytsii-zsu-na-skhodi-krainy-video>

<sup>135</sup> SSU, “SSU neutralizes over 160 enemy sabotage groups and declares 1,000 persons suspects in cases on crimes against state security (video),” *News*, 8 June 2022, accessed 10 June 2022, <https://ssu.gov.ua/en/novyny/sbu-vykryla-ponad-160-vorozhykh-drh-i-povidomyla-pro-pidozry-1-tys-zlovmysnykiv-za-zlochyny-proty-derzhbezpeky-video>

<sup>136</sup> SSU, “Every day SSU eliminates enemy agent networks, detects spies and saboteurs,” *News*, 10 March 2022, accessed 2 June 2022, <https://ssu.gov.ua/en/novyny/sbu-shchodnia-zatrymuie-ta-likvidovuiie-ahenturni-merezhi-voroaha-vyivliaie-shpyhuniv-i-dyversantiv>

<sup>137</sup> SSU, “SSU’s official statement on collaboration of Ukrainians with enemy,” *News*, 14 March 2022, accessed 2 June 2022, <https://ssu.gov.ua/en/novyny/ofitsiina-zaiava-sbu-shchodo-spivpratsi-ukraintsiv-z-vorohom>

<sup>138</sup> SSU, “Every day SSU eliminates enemy agent networks,...”

<sup>139</sup> SSU, “SSU neutralizes over 160 enemy sabotage groups ...”

<sup>140</sup> Mick Krever, “Ukraine’s security service hunts the spies selling information to Russia,” *CNN News*, 16 May 2022, updated 17 May, accessed 17 May 2022, <https://edition.cnn.com/2022/05/16/europe/ukraine-sbu-russian-spies-intl/index.html>

<sup>141</sup> 戦時下に敵を公然と支持し或いは称賛する資料の作成配布は刑法 436 条の 2 によって犯罪となる。Yaroslav Trofimov, “Ukraine Security Services Hunt for Russia Supporters and Agents in Their Midst”, *The Wall Street Journal*, [https://www.wsj.com/articles/ukraine-security-services-hunt-for-russia-supporters-and-agents-in-their-midst-11654161968?mod=panda\\_wsj\\_custom\\_topic\\_alert](https://www.wsj.com/articles/ukraine-security-services-hunt-for-russia-supporters-and-agents-in-their-midst-11654161968?mod=panda_wsj_custom_topic_alert)

### ① 典型的なスパイ団の摘発（2022年7月）

2022年7月のSSU広報<sup>142</sup>によれば、GRUのスパイ団4人を摘発した。スパイ団はキーウ、チェルニーヒウ地区担当のGRUドネツ大佐によって創設されたもので、首謀者は「ルハンスク自治共和国」国家安全省の職員ティリリムであった。4人中2人が情報収集担当で、キーウ周辺の軍部隊と重要施設の位置情報やウクライナ軍将校や法執行職員の個人情報を収集していた。残り2人は親ロシア宣伝をインターネットを通じて行っていたものである。

### ② 標的情報を提供する作業者・協力者の摘発

SSUによる検挙事例では、標的情報を提供する作業者や協力者の事例が最も多い。戦争中であるので、当然のことであろう。ロシア軍に標的情報を送った検挙事例として注目すべき事件には次の事例がある。数例を紹介する。

#### ○ ヤヴォリウ訓練場の標的情報の提供者の摘発（2022年6月）

2022年6月のSSU広報<sup>143</sup>によれば、ウクライナ西部ヤヴォリウ訓練場の標的情報を提供した元KGB将校のロシア軍協力者が6月下旬に検挙された。ロシア軍は3月13日訓練場を巡航ミサイル多数で攻撃して、死者61人負傷者147人という大きな被害を与えたが、元KGB将校はテレグラム通信アプリを使用して正確な位置情報など攻撃に必要な標的情報を送っていた。また、同じく6月下旬、首都キーウでミサイル攻撃の標的情報と効果測定情報（写真）を送っていたロシア作業者を摘発した。

#### ○ SSU施設の標的情報の提供者の摘発（2022年11月）

2022年11月のSSU広報<sup>144</sup>によれば、南部ミコライウ市の住民で匿名のテレグラム通信を使って標的情報を送っていた住民を摘発した。住民は、侵攻開始後にSNSで積極的にロシアを支持する意見を発信していたところをリクルートされたものであり、逮捕時には、ロシア軍がミサイル攻撃の標的とするミコライウ市内のSSU施設の正確な座標情報を送信しようとしていた。

### ③ 破壊活動の摘発

敵支配地域内で破壊活動を行うのは戦争における常套手段であるが、これを抑止して後方

---

<sup>142</sup> SSU, “SSU detains agents of russian GRU who collected intelligence on Kyiv’s defence (video),” *News*, 1 July 2022, accessed 2 July 2022, <https://ssu.gov.ua/en/novyny/sbu-zneshkodyla-ahenturnu-hrupu-hru-rf-yaka-zbyrala-rozviddani-shchodo-oborony-kyieva-video>.

<sup>143</sup> SSU, “SSU detains individuals who adjusted enemy missile strikes in Kyiv, Lviv and Donetsk regions (video),” *News*, 28 June 2022, accessed 29 June 2022, <https://ssu.gov.ua/en/novyny/sbu-zatrymala-koryhuvalnykiv-vorozhykh-raketnykh-udariv-polivshchyni-kyievu-ta-donechchyni-video>

<sup>144</sup> SSU, “SSU detains forward observer who ‘guided’ russian missiles at SSU building in Mykolaiv,” *News*, 8 November 2022, accessed 10 November 2022,

<https://ssu.gov.ua/en/novyny/sluzhba-bezpeky-zatrymala-koryhuvalnyka-yakyi-navodyv-rosiiski-rakety-po-budivli-sbu-u-mykolaievi>

治安を確保するのもセキュリティ・サービスの重要な任務の一つである。

#### ○ 侵攻前の破壊活動の摘発（検挙 2022 年 1 月、有罪判決 7 月）

2022 年 7 月の SSU 広報<sup>145</sup>によれば、ロシア GRU 作員がテロ行為によって 8 年の拘禁刑と財産没収の判決を受けた。本作員は、ウクライナの西方にある沿ドニエストル共和国内を工作基地とする GRU の指示を受け、定期的にウクライナを訪問してきた。作員の任務は、ロシア軍の全面侵攻に先立ち破壊活動やテロを行って、オデーサ地方は反ウクライナ感情が強く親ロシア地下組織が存在するという印象を作り出すことであった。そのため作員は、2021 年 12 月にはウクライナ軍車両への放火や英雄記念碑の破壊を組織した。更に、軍事装備や愛国的社会組織への攻撃を組織しようとして、1 月初旬実行者をリクルートしようとしているところを現行犯で検挙された。（広報文から判断して、通信傍受或いは捜査によって検挙したことが推定できる。）

#### ○ 開戦直後キーウにおける破壊活動、大統領暗殺の阻止（2022 年 2 月）

開戦直後、ロシア軍は、首都キーウに混乱に陥れ、大統領を除去するため、事前に潜入させた作員による破壊活動や大統領暗殺の企てを敢行したという。その詳細は未だに明らかになっていないが、主としてセキュリティ・サービス SSU が特殊部隊アルファも使用して、破壊活動や大統領暗殺を阻止したとされる<sup>146</sup>。

#### ○ 国防相、軍情報局長暗殺の未然防止（2022 年 8 月）

2022 年 8 月の SSU 広報<sup>147</sup>によれば、ロシア占領地のルハンスク州の住民で GRU の協力者は、GRU の指示に従い、ウクライナの犯罪者を金で雇ってウクライナ軍人を暗殺させようと企図して、ベラルーシを経由してウクライナに入ったところを犯罪者ともども検挙された。当初の暗殺は「腕試し」（テスト）であって、暗殺の本命は、国防相と軍情報局長で、報酬は 10 万ドルから 15 万ドルが提示されていたという。

#### ○ 破壊活動の未然防止（検挙 2022 年 10 月）

2022 年 11 月の SSU 広報によれば<sup>148</sup>、GRU 協力者が、オデーサ地区の鉄道による軍需輸送状況の情報収集を行い、鉄道爆破の破壊活動を計画していたところを検挙された。同人は元警察官で、侵攻当初に GRU の協力者になった。鉄道線路沿いに無線カメラを仕掛けてリアル・タイムに情報収集をし、また、鉄道線路爆破のために TNT 火薬や対

---

<sup>145</sup> SSU, “SSU: russian agent who planned terrorist attacks in Odesa region sentenced to 8 years in prison, *News*, 13 July 2022, accessed 15 July 2022, <https://ssu.gov.ua/en/novyny/sbu-do-8-rokiv-uviaznennia-zasudzheni-ahenta-rf-yakyi-hotuvav-terakty-na-odeshchyni>

<sup>146</sup> 大統領の立て籠る大統領府地下施設への侵入未遂など、暗殺の企図は 13 回にも及んだとされる。大統領府周辺は主として SSU 特殊部隊アルファが警備を固めて防衛した。前掲「NHK スペシャル『ウクライナ大統領府 軍事侵攻・緊迫の 72 時間』」

<sup>147</sup> SSU, “SSU detains russian killers who planned to assassinate Minister of Defence and Head of Military Intelligence,” *News*, 8 August 2022, accessed 12 August 2022, <https://ssu.gov.ua/en/novyny/ssu-detains-russian-killers-who-planned-to-assassinate-minister-of-defence-and-head-of-military-intelligence-video>

<sup>148</sup> SSU, “SSU detains saboteur of russian military intelligence who prepared explosions on Odesa railway,” *News*, 1 November 2022, accessed 4 November 2022, <https://ssu.gov.ua/en/novyny/sbu-zatrymala-dyversanta-rosiiskoi-voiennoi-rozvidky-yakyi-hotuvav-vybukhy-na-odeskii-zaloznytsi-video>

戦車地雷を保持していた。

#### ○ 特殊部隊指揮官の暗殺の阻止（検挙 2022 年 11 月）

2022 年 11 月の SSU 広報によれば<sup>149</sup>、FSB の偵察・破壊活動グループを摘発した。彼らは FSB によってリクルートされ、首都と北東部におけるウクライナ部隊の配置移動状況について偵察活動を行っていたが、特に軍特殊部隊の指揮官たちの個人情報と所在情報の収集に力を入れていた。SSU は彼らの活動を発見し、彼らが隠匿場所から武器（対戦車地雷、手榴弾、自動小銃）を取り出そうとしている現場で検挙した。

#### ④ 軍関係のスパイの摘発

##### ○ 元軍情報局次長（少将）の摘発（2022 年全面侵攻後早期、公表 8 月）

2022 年 8 月の SSU 広報<sup>150</sup>によれば、ロシア軍の全面侵攻開始後早々に元ウクライナ軍情報局副局長（少将）を拘束した。犯罪容疑は、ロシア諜報機関にウクライナの軍事情報や政治情報を提供していたことである。同少将は、2008 年から 2010 年までウクライナ軍情報局副局長を務め、その後も政府機関で勤務していたが、ソ連時代にフルンゼ軍事大学やモスクワ高級軍事指揮学校で学んだ経験から親ロシア感情をもっていた。同少将は拘束に向かったセキュリティ・サービスの将校に対してマカロフ軍用拳銃を射撃して抵抗したため、国家反逆罪、法執行職員に対する攻撃、武器の不法所持の罪名の通告を受けた。

##### ○ 下級レベルにおけるスパイの摘発（2023 年 6 月）

ウクライナ軍の下級レベルにおいても、浸透したスパイの摘発が続いている。例えば 2023 年 6 月に公表された事案を見ると次の通り。なお、ウクライナ軍内のスパイ摘発の広報は 2022 年中は殆ど見なかったが、2023 年になって広報が増えている。ウクライナ軍の反攻を前にして、作戦保全のため軍内スパイの検挙活動を強化している可能性がある。

- ・ SSU 軍防諜部は、軍指導部の支援を受けて、ドニプロペトロウシク州で多様な特別作戦を実施した。その結果、軍内の GRU スパイを摘発した。スパイはザポリージャ州出身であるが、ロシア軍全面侵攻前に入隊してドニプロペトロウシク州の駐屯地で勤務していた。2022 年後半にリモートで GRU にリクルートされ、ウクライナ軍の作戦計画に関する情報を収集していた。ウクライナ軍の反転攻勢の開始（2023 年 6 月）を前にして、スパイは、ウクライナ軍の反攻の開始日と主攻正面、外国製の武器装備の前線への輸送経路に関する情報を収集するように緊急指令を受けた。また、スパイはウクライナ軍の無線通信チャンネルを特定しようとしていた。SSU は、スパイが情報収集活動をしている所を拘束したのである。

---

<sup>149</sup> SSU, “SSU detains enemy reconnaissance and sabotage group that prepared assassinations of Ukrainian SOF commanders,” *News*, 9 November 2022, accessed 10 November 2022, <https://ssu.gov.ua/en/novyny/sbu-zneshkodyla-vorozhu-drh-yaka-hotuvala-vbyvstva-komandyriv-syl-spetsialnykh-operatsii-zsu-video>

<sup>150</sup> SSU, “SSU notifies former deputy head of Ukraine’s military intelligence of suspicion of treason (video),” *News*, 5 August 2022, accessed 8 August 2022, <https://ssu.gov.ua/en/novyny/sbu-povidomya-pro-pidozru-u-derzhavnii-zradi-kolyshnomu-zastupnyku-holovy-hur-mou-video>

スパイは、占領地に残った母親を通じて GRU から接触を受け、その後テレグラム通信を使用して、直接 GRU 作業員と通信していた<sup>151</sup>。

- SSU 軍防諜部は、ジトーミル州で特殊作戦を実施して軍内の FSB スパイを摘発した。スパイは、空港（複数）の状態や戦闘機による使用状況を調査し、弾薬や燃料の備蓄場所の情報を送っていたが、更に MaxxPro 装甲戦闘車の基地と動きを捕捉しようとしていた。スパイは、地元出身でウクライナ北部の駐屯地に勤務していたところ、2023 年 5 月に FSB にインターネットを介してリクルートされ、テレグラム通信を使って交信をしていた。スパイは、自分でジトーミル州の各地の軍施設を偵察すると共に、知人からも情報を収集しようとしていた。SSU はスパイが偵察活動をしているところを拘束して、携帯電話を押収した<sup>152</sup>。

二つの事例とも、戒厳令下の国家反逆罪であり終身刑の可能性がある。

#### ⑤ SSU 内のスパイの摘発と暴露<sup>153</sup>

##### ○ オレグ・クリニッチ：SSU クリミア州支局長（2022 年 3 月解任。7 月逮捕）

侵攻 3 時間前にクリミアのロシア軍の侵攻切迫の兆候情報を得たが、これを SSU 本部

---

<sup>151</sup> SSU, “SSU detains russian mole in Ukrainian Armed Forces who intended to ‘leak’ directions of Ukraine’s counteroffensive to ruscists,” *News*, 14 June 2023, last accessed 31 July 2023, <https://ssu.gov.ua/en/novyny/sbu-zatrymala-rosiiskoho-krota-u-lavakh-zsu-yakyi-khotiv-zlyty-rashystam-napriamky-ukrainskoho-kontrnastupu>

<sup>152</sup> SSU, “SSU detains another mole in Ukraine’s Armed Forces who spied on Ukrainian combat aircraft and MaxxPro fighting vehicles,” *News*, 23 June 2023, last accessed 31 July 2023, <https://ssu.gov.ua/en/novyny/sbu-zatrymala-shche-odnoho-krota-v-zsu-yakyi-shpyhuvav-za-ukrainskymy-boiovymy-litakamy-i-bronemashynamy-maxxpro>

<sup>153</sup> “How Russia Spread a Secret Web of Agents Across Ukraine,” *Reuters*, 30 July 2022, accessed 1 August 2022, <https://www.voanews.com/a/how-russia-spread-a-secret-web-of-agents-across-ukraine/6677718.html>

-- Greg Miller and Catherine Belton, “Russia’s spies misread Ukraine and misled Kremlin as war loomed,” *The Washington Post*, 19 August 2022, accessed 19 August 2022, <https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/?itid=hp-top-table-main-t-2>

--Joseph Choi, “Zelensky: Two Ukrainian generals dismissed for being ‘traitors,’” *The Hill*, 31 March 2022, accessed 21 August 2022, <https://thehill.com/policy/international/3256034-zelensky-two-ukrainian-generals-dismissed-for-being-traitors/>

--“Map of minefields of Kherson region was handed over to Russians by traitor from SSU Sadokhin, - chairman of regional council Samoilenko,” *CENSOR.NET*, 18 June 2022, accessed 21 August 2022, <https://censor.net/en/n3348767>

--“Zelenskyy replaces long-time loyalists with Yermak’s people,” *Yahoo News*, 20 July 2022, 21 August 2022, <https://news.yahoo.com/zelenskyy-replaces-long-time-loyalists-173500464.html>

--Oleksiy Yarmolenko, “The Prosecutor General’s Office made public the details of the case of the ex-head of the Crimean SSU Kulinich. He was recruited by the FSB, and his accomplice was the ex-deputy secretary of the National Security Council,” *Babel ua*, 23 July 2022, accessed 21 August 2022, <https://babel.ua/en/news/81904-the-prosecutor-general-s-office-made-public-the-details-of-the-case-of-the-ex-head-of-the-crimean-ssu-kulinich-he-was-recruited-by-the-fsb-and-his-accomplice-was-the-ex-deputy-secretary-of-the-nationa>

に報告しなかったため、ウクライナ軍の対処準備が遅れ、ロシア軍の南部での進軍を容易にしたとされる。遅くも2019年6月以来FSBの協力者であり、SSUの内部情報を提供してきた。また後述のナウモフの防諜部長就任の裏工作など、SSU内の人事に影響を与えた。

2022年3月2日に解任。7月16日に拘束される。7月17日ゼレンスキー大統領は竹馬の友であったSSU長官のバカノフを突然解任したが、その一因はバカノフがクリニチを重用するなど、SSU内のスパイ対策が不十分であったこととされている。

○ セルヒイ・クリヴォルチュコ：SSUヘルソン州支局長（2022年3月解任。拘束時期不明）

ロシアの全面侵攻に直面して、部下に無抵抗を指示したとされる。2022年3月末解任。国家反逆罪で起訴。部下の支局幹部イゴル・サドキンは、ロシア軍に地雷原の地図他の軍事情報を提供し協力したとして、同じく3月に逮捕されている。SSUヘルソン州支局の機能不全が、ロシア軍がヘルソン州を容易に占領した要因と見られている。

○ アンドリイ・ナウモフ：SSU本部防諜部長（2022年2月逃亡。6月セルビアで逮捕）

チェルノブイリ原発警備に関する機密情報を漏洩したとされる。2022年3月末解任。ロシア軍の侵攻開始直前の2月23日に逃亡したが、6月にセルビア国境で逮捕。現金13万ドルと60万ユーロ以上と宝石エメラルド2個を所持していた。

○ 下級レベルにおける浸透スパイの摘発（2022年11月）

SSUの下級レベルにおいても、浸透したスパイの摘発も並行的に進んでいる。例えば、2022年11月に公表された事案を見ると次の通り。

- ・ 2022年11月ハルキウ州SSU支局の他機関調整担当職員が起訴されている。同人はロシア侵攻開始直後に、ウクライナ敗北後の自分と家族の安全の保証と引き換えに、GRUに協力を始め、ウクライナ軍の人員装備の配置移動情報、作戦活動情報などを提供していた。同人とロシアGRU担当者間の通信傍受から発覚したようである<sup>154</sup>。
- ・ 同11月、二重スパイになる目的で、SSUに協力したいと接近してきたFSB協力者の女性を、暴露して逮捕した。SSUは女性が2019年以来ロシア側協力者であったことを探知していたようである<sup>155</sup>。

⑥ 政府・政治家のスパイ摘発

○ 内閣官房のスパイ摘発（2022年6月）

2022年6月のSSU広報<sup>156</sup>によれば、SSUは内閣官房の幹部職員とウクライナ商工会

---

<sup>154</sup> SSU, “SSU completes investigation of case on russian ‘mole’ in Kharkiv SSU Office” *News*, 2 November 2022, accessed 4 November 2022, <https://ssu.gov.ua/en/novyny/sbu-zakinchyla-rozsliduvaty-spravu-krota-fsb-yakyi-znakhodyvsia-u-kharkivskomu-upravlinni-sluzhby-bezpeky>

<sup>155</sup> SSU, “SSU detains fsb spy who tried to infiltrate SSU and become ‘double agent’,” *News*, 2 November 2022, accessed 4 November 2022, <https://ssu.gov.ua/en/novyny/sluzhba-bezpeky-zatrymala-shpyhunku-fsb-yaka-namahalasia-pronyknuty-v-sbu-i-staty-podviinym-ahentom-video>

<sup>156</sup> SSU, “SSU exposes russian agent network which included officials of Cabinet of Ministers and Chamber of Commerce and Industry of Ukraine (video),” *News*, 21 June 2022, accessed 22

議所幹部職員を逮捕した。内閣官房の幹部職員は、2012年にロシア旅行をした際ロシアFSBによってリクルートされ、秘密情報を1件2千ドルから1万5千ドルで売っていた。彼は、官房でアクセスできる防衛力、国境管理、治安職員の個人データなどを入手してUSBメモリーで持ち出し、これをテレグラム通信アプリを使って商工会議所職員を經由してFSBに提供していたものである。検挙に至る過程は公表されていないが、SSUが通信傍受能力を含めて極めて強力な情報収集力を有することが伺われる。(2022年8月に懲役12年、全財産没収の判決を受けた<sup>157</sup>。)

#### ○ 国会議員デルカッチの摘発 (2022年6月)

2022年6月のSSU広報<sup>158</sup>によれば、SSUは有力政治家で国会議員のアンドリイ・デルカッチと秘書をロシアGRUのスパイとして摘発した。デルカッチは2016年にリクルートされ、現GRU長官イゴール・コステュコフと副長官のウラディミール・アレクセーエフの指示を受けて働いていた。ウクライナ戦争での任務は、ロシア占領軍に協力する民間警備組織の設立であり、このため数か月毎に3~4百万ドルを受領していたとされる。SSU広報では、デルカッチとアレクセーエフ副長官の電話通信傍受記録が開示されている。

なお、デルカッチは2020年米大統領選挙で、ロシアの意向を受けバイデン大統領候補者(当時)を誹謗中傷する情報を流し選挙干渉をしたことでも知られている。

#### ○ 国会議員秘書の摘発 (2022年7月)

2022年7月のSSU広報<sup>159</sup>によれば、国会議員の政策秘書をFSB協力者であるとして国家反逆罪で摘発した。政策秘書はモスクワ旅行をした際にFSB第5総局員にリクルートされ、その後第5総局幹部の指示を受け、暗号化電子通信によって情報を送っていた。FSB運営者とは第三国で会談して指示を受けていたが、報酬は情報と任務内容に応じて、月1500~4000ドルであった。

#### ⑦ 被占領地域でのロシア軍への協力者の公表 (2022年7月) と摘発

被占領地域でロシアに積極的に協力することは対敵協力の犯罪となるとして、協力者を積極的に公表して、警告を発している。

一例を挙げると、被占領地で占領軍が設置したロシア「内務省ヘルソン州局」と傘下の民兵組織は住民の抵抗運動を弾圧し住民を虐待しているとして、その職員26人を特定し、彼

---

June 2022, <https://ssu.gov.ua/en/novyny/sbu-vykryla-rosiisku-ahenturu-do-yakoi-vkhodyly-posadovtsi-kabminu-i-torhovopromyslovoi-palaty-ukrainy-video>

<sup>157</sup> SSU, "Following SSU's investigation, FSB's mole in Ukraine's Cabinet of Ministers will spend 12 years in prison," *News*, 25 August 2022, accessed 28 August 2022, <https://ssu.gov.ua/en/novyny/za-materialamy-sbu-krit-fsb-u-kabmini-provede-12-rokiv-za-gratamy>

<sup>158</sup> SSU, "SSU exposes agent network of russian GRU which included Ukrainian MP (video)," *News*, 24 June 2022, accessed 25 June 2022, <https://ssu.gov.ua/en/novyny/sbu-vykryla-ahenturnu-merezhu-hru-rf-do-yakoi-vkhodyv-narodnyi-deputat-ukrainy-video>

<sup>159</sup> SSU, "SSU exposes assistant to MP on treason (video)," *News*, 5 July 2022, accessed 7 July 2022, <https://ssu.gov.ua/en/novyny/sbu-vykryla-na-derzhavnii-zradi-pomichnyka-narodnoho-deputata-ukrainy-video>

らに対して対敵協力罪容疑を通告した（26人中14人は元ウクライナ国家警察職員）。その上、幹部10人の氏名と写真をウェブサイトで公表した<sup>160</sup>。ロシアは占領地域の併合を視野に入れてロシア化を進めていた。公表は、これに協力する行為にブレーキを掛けようとしてのことであろう。

なお、ウクライナ軍は、2022年9月以降、反転攻勢を始め、ロシア軍による占領地の一部を奪還している。占領奪還地では、住民から情報を収集して、ロシア占領当局に対する積極的協力者の特定と摘発や起訴を進めている<sup>161</sup>。

以上から分かるように、ロシア諜報機関は作業者や協力者を使って、侵攻前の破壊活動、軍・インテリジェンス機関・政治家への浸透、標的情報の収集など幅広い活動を行っており、これら作業者や協力者の摘発無害化は、戦時国家においては必須の機能である。

### ⑧ 戦争犯罪の捜査・起訴の状況（2023年6月）

2023年6月のSSU広報はマリュークSSU長官の発言を伝えているが<sup>162</sup>、次の通り。

SSUはロシア軍による全面侵攻が始まって以来、戦争関連で9万2千件近くの刑事手続を開始した。その内、4万3千件は国際戦闘法規の違反である。主眼はロシアの軍事政治指導部員であり、指導部の司令官25人以上を含む448人の戦争犯罪人に対して容疑を通告している。犯罪人個人を特定しており、例えば、ある重爆撃連隊の隊長ティモシン大佐は、2022年6月のポルタヴァ州クレメンシュグ市のアムストール・ショッピングセンターと2023年1月のドニプロペトロウシク州ドニプロ市の住宅ビルに対するミサイル攻撃の容疑である。（註：これらの攻撃で多数の民間員死傷者が出ている。）更に、これら448人の内、95件で142を起訴しており、既に22人に対して有罪判決が出ている。（註：有罪判決は欠席裁判である可能性が高い。）

これらの捜査においては、国際組織も関与しており、SSU自体は、現場鑑識の他、オー

---

<sup>160</sup> SSU, "SSU identifies all collaborators and traitors who joined 'ministry of internal affairs of russia' in Kherson region (video)," *News*, 25 July 2022, accessed 25 July 2022, <https://ssu.gov.ua/en/novyny/sbu-identyfikoval-a-vsikh-kolaborantiv-i-zradnykiv-yaki-vstupyly-do-okupatsiinoho-mvd-rf-na-khersonshchyni-video>.

<sup>161</sup> SSU, "SSU 'cracks' enemy accomplices in de-occupied Luhansk region, who provided ruscists with information on Ukrainian patriots and IDPs," *News*, 15 November 2022, accessed 17 November 2022, <https://ssu.gov.ua/en/novyny/sbu-rozkolola-vorozhykh-poplichnyts-na-deokupovanii-luhanshchyni-yaki-zdavaly-okupantam-dani-pro-ukrainskykh-patriotiv-ta-pereselentsiv>

--- SSU, "SSU calls on Ukrainians to report traitors and collaborators in Mykolaiv and Kherson regions," *News*, 15 November 2022, accessed 17 November 2022, <https://ssu.gov.ua/en/novyny/sbu-zaklykaie-ukrainsiv-povidomliaty-pro-zradnykiv-i-kolaborantiv-na-mykolaivshchyni-ta-khersonshchyni>

<sup>162</sup> SSU, "SSU opened almost 92,000 criminal proceedings on Russia's full-scale aggression - Vasyl Maliuk," *News*, 21 June 2023, last accessed 31 July 2023, <https://ssu.gov.ua/en/novyny/sbu-rozpochala-rozsliduvannia-maizhe-92-tys-kryminalnykh-provazhzen-shchodo-povnomasshtabnoi-ahresii-rf-vasyl-maliuk>



プリンソース分析やソフトウェアの使用、軍や検事局との連携を図っている。SSU は証拠の収集分析作業を統合しており、ミサイルの断片、傍受通信、衛星画像、鹵獲資料 (trophy documentation) など証拠となるものは全て収集している。

祖国防衛戦争においては、侵略者による戦争犯罪の捜査まで視野に入れて対処する必要があるが、それにはどれだけの準備が必要か、考えさせられる。

## (5) サイバー攻撃対策

ウクライナのサイバーセキュリティ対策は、国家安全保障・国防会議に附置されたサイバーセキュリティ国家調整センター (National Coordination Center for Cybersecurity) の統括の下、デジタル変革省、特殊通信・情報保護庁、SSU など幾つかの組織が協力して当たっている。

特殊通信・情報保護庁は、国家の通信システムを提供管理しているほか、コンピューター緊急対応チーム CERT-UA (Computer Emergency Response Team) を設置して、サイバー攻撃事案の収集分析、サイバー攻撃防止技術の提供、セミナー開催、サイバー攻撃・脅威に対抗するための勧告など、全般的なサイバーセキュリティ対策を担当している<sup>163</sup>。

これに対して SSU は、主として外国諜報機関による標的型サイバー攻撃対策を担当し、通信傍受などによるアクティブなサイバーセキュリティ対策も遂行している。このため SSU は、サイバーセキュリティ状況センター (Cyber Security Situation Centre) を設置して 24 時間監視態勢を敷いて対処している。SSU の活動を公表資料に拠って見てみよう<sup>164</sup>。

ウクライナに対するサイバー攻撃は、ロシアでは主として FSB と GRU が担当しており、実際の攻撃は各種ハッカー集団 APT28 (Fancy Bear)、APT29 (Cozy Bear)、Sandworm、Berserk Bear、Gamaredon、Vermin 他が実行している<sup>165</sup>。SSU の広報資料<sup>166</sup>に拠れば、攻撃は、開戦前から始まり、2022 年 1 月 13 日 14 日<sup>167</sup>、2 月 15 日 16 日と 2 波の大規模攻撃があり、更に全面侵攻開始時の 2 月 23 日 24 日に大規模攻撃があった。全面進攻時の攻撃対象は、通信、エネルギー、運輸という重要インフラを麻痺させるため、そ

<sup>163</sup> CERT-UA, accessed 22 October 2022, <https://cert.gov.ua/about-us>

<sup>164</sup> SSU, accessed 22 October 2022, <https://ssu.gov.ua/en>

公刊資料から判断する限り、特殊通信・情報保護庁は国家の通信システムの提供管理を主として担い、通信傍受などによるアクティブなサイバーセキュリティ対策は SSU が所掌していると思われる。State Service of Special Communications & Information Protection – Ukraine, website.

<sup>165</sup> SSU, “SSU: On night of full-scale invasion, Russia aimed to destroy all cyber defence of Ukraine (video),” *News*, 2 April 2022, accessed 1 June 2022, <https://ssu.gov.ua/en/novyny/u-nich-povnomasshtabnoho-vtorhnennia-rf-voroh-khotiv-znyshchyty-ves-kiberzakhyst-ukrainy-sbu-video>

<sup>166</sup> SSU, “SSU steps up cyber defence of strategic facilities and creates emergency email,” *News*, 8 March 2022, accessed 2 June 2022, <https://ssu.gov.ua/en/novyny/sbu-posyliuie-kiberzakhyst-stratehichnykh-objektiv-i-stvoriuie-dlia-tsoho-hariachu-elektronnu-adresu>

<sup>167</sup> 1 月の攻撃は、「ワイパー」という破壊的ウィルスによるもので、政府系の 70 のサイトが攻撃され機能不全となったという。ウクライナ政府はスロバキアの IT 企業 ESET に解析を依頼した。

—「ウクライナ・サイバー戦 “見えない”戦争の実態」NHK クローズアップ現代、2022 年 6 月 27 日放送。

これらの情報通信システムを狙ったものであった<sup>168</sup>。また、「フォックス・ブレード」という破壊的ウイルスによる政府システムに対する攻撃もあった<sup>169</sup>。しかし、SSU と関係機関の迅速な対応により事無きを得たとしている。

その後も政府機関、通信事業、マスメディア等を標的とした攻撃は続いているが、SSU はサイバーセキュリティ状況センターで 24 時間監視態勢を敷いて対処しており、EU 及び NATO 諸国の担当者との情報交換もして対処している。

対処の成果は、2022 年の全面侵攻以来同年 6 月 6 日までに、サイバー事案・サイバー攻撃 827 件を阻止し又は無力化したとしている。その内容には、CC サーバーへの接続 69 件、侵入行為 46 件、弱点利用 25 件、マルウェア感染 59 件などがある<sup>170</sup>・<sup>171</sup>。また、全面侵攻開始から 2022 年 10 月 3 日までに、政府及び重要インフラ企業に対するサイバー攻撃 3500 件以上を探知し無力化したとしている。この内 1650 件の攻撃は SSU のセキュリティ情報事案対処システムがリアル・タイムで探知して阻止している。また、主たる攻撃目標は、政府の通信システムと、エネルギーと運輸部門の重要戦略企業の妨害破壊である<sup>172</sup>。更に 2022 年 9 月以降ウクライナ軍が反転攻勢に転じたが、これに対抗してロシア軍は、発電所などの生活インフラへの攻撃を激化させている。インフラ攻撃では、ミサイルなどによる物理的攻撃と併せて、サイバー攻撃が毎日 10 件以上と多用されているが、SSU がサイバー攻撃の多くは阻止しているとしている<sup>173</sup>。

---

<sup>168</sup> 2 月 24 日の通信分野の攻撃では、ウクライナ軍も広汎に使用していた衛星通信 KA-SAT の通信機の部品モデムがハッキングされており、開戦当日に大規模な通信障害を起し、通信容量が 20% までに激減した。ウクライナのフェドロフ・デジタル相が緊急にイーロン・マスクにスターリンク衛星通信の提供を要請した背景が理解できる。Ellen Nakashima, “Russian military behind hack of satellite communication devices in Ukraine at war’s outset, U.S. officials say,” *The Washington Post*, 24 March 2022, accessed 5 June 2022, “<https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/>”

-- 「ウクライナ・サイバー戦 “見えない”戦争の実態」NHK クローズアップ現代。

<sup>169</sup> Microsoft, *ibid.*, p.7.

<sup>170</sup> SSU, “Since start of russia’s full-scale aggression, SSU thwarts and neutralizes over 800 cyberincidents and cyberattacks,” *News*, 6 June 2022, accessed 10 June 2022, <https://ssu.gov.ua/en/novyny/za-chas-povnomasshtabnoi-ahresii-sbu-poperedyla-ta-neitralizuvala-ponad-800-kiberintsydentia-ta-kiberatak>

-- SSU, *Information Security Protection*, 6 June 2022, accessed 10 June 2022, <https://ssu.gov.ua/en/zabezpechennia-informatsiinoi-bezpeky>

<sup>171</sup> 2022 年 6 月 28 日の憲法記念日を前に、ロシア諜報機関がウクライナのテレビ放送システムへの侵入の試みだが、これを探知して阻止したと広報している。SSU, “SSU prevents russian special services from hacking Ukrainian TV channels participating in national telethon,” *News*, 28 June 2022, accessed 29 June 2022, <https://ssu.gov.ua/en/novyny/sbu-ne-dala-rosiiskym-spetssluzhbam-zlamaty-ukrainski-telekanaly-yaki-berut-uchast-u-natsionalnomu-telemarafoni>

<sup>172</sup> SSU, “SSU neutralizes almost 3,500 cyberattacks on government authorities and infrastructure facilities since war started,” *News*, 3 October 2022, accessed 20 October 2022, <https://ssu.gov.ua/en/novyny/z-pochatku-viiny-sbu-neitralizuvala-maizhe-35-tys-kiberatak-na-orhany-vlady-ta-obiekty-infrastruktury>

<sup>173</sup> SSU, “russia carries out over 10 cyberattacks on Ukraine’s strategic facilities daily – Chief of

こうして、サイバー事案・サイバー攻撃の阻止・無力化の件数は、2022年1年間では4500件以上で、2021年の1400件、2020年800件と比べて大幅に増加している<sup>174</sup>。

またSSUは、システム上でサイバーセキュリティ対策を講じているだけではなく、セキュリティ・サービスとしての特性を活かして、ウクライナ国内の現場でもロシアによるサイバー攻撃に加担している者を検挙している。検挙事例として公表されているのは、ウクライナ国内からDDOS攻撃を行うハッカー集団の検挙、偽情報の大規模発信拠点の「ボットファーム」の検挙、親ロシア情報を拡散するSNS集団の検挙などが挙げられている<sup>175</sup>。2022年10月3日のSSU広報によれば、攻撃の準備段階での検挙事例もあり、通信傍受などを駆使して被害を未然防止して姿も浮かび上がってくる<sup>176</sup>。

なお、SSUは、2022年4月NATOのサイバー脅威の情報共有組織に参加したと発表した。同計画は、2012年に発足した「多国間マルウェア情報共有プラットフォーム(MISP)」で、重要インフラ、政府、軍関係施設1300以上の代表が参加するマルウェア情報の共有組織である<sup>177</sup>。

## (6) 情報作戦

今回のロシア・ウクライナ戦争に関しては、米国を初め各国による情報作戦が遂行されている。ウクライナでも大統領初め情報作戦を遂行しているが、SSUもウェブサイトでの広報や検挙活動によって情報作戦の一翼を担っている。

### ア SSUによる情報作戦

先に(2)アで幾つかの事例を紹介したが、主としてロシア兵の電話通話の内容をSSUサイトで公開することにより、ロシア軍の残虐性や戦争犯罪を糾弾広報してウクライナへの支援気分を醸成し、或はロシアの指揮兵站の酷さを広報してロシア軍内での厭戦気運を醸成しようとしている。幾つかを紹介する。

- ロシア軍兵士と妻との電話通話：妻にウクライナ女性の強姦の承認を求めたのに対して、妻が避妊具を使えと話している状況<sup>178</sup>。夫婦の会話が冗談か本気か不明であるが、広

---

SSU Cyber Security Department,” *News*, 9 November 2022, accessed 13 November, <https://ssu.gov.ua/en/novyny/rf-shchodnia-zdiisniuiie-ponad-10-kiberatak-na-stratehichni-objekty-ukrainy-kerivnyk-departamentu-kiberbezpeky-sbu>

<sup>174</sup> SSU, “SSU neutralized over 4500 cyberattacks on Ukraine in 2022-Liia Vitiuk”, *News*, 26 December 2022, accessed 3 January 2023, <https://ssu.gov.ua/en/novyny/z-pochatku-roku-sbu-neutralizovala-ponad-45-tys-kiberatak-na-ukrainu-illia-vitiuk>

<sup>175</sup> SSU, “SSU prevents cyber attacks on government and sends to court case against Shariy’s accomplice who supported russian aggression (video),” *News*, 2 June 2022, accessed 5 June 2022, <https://ssu.gov.ua/en/novyny/sbu-zapobihla-serii-kiberatak-na-orhany-vlady-i-peredala-do-sudu-spravu-shchodo-poplichnytsi-shariia-yaka-vypravdovuvala-ahresiiu-rf-video>

<sup>176</sup> SSU, “SSU neutralizes almost 3,500 cyberattacks on government authorities and infrastructure facilities since war started.”

<sup>177</sup> SSU, “SSU and NATO step up cooperation in cybersecurity: threat monitoring systems integrated,” *News*, 5 April 2022, accessed 1 June 2022, <https://ssu.gov.ua/en/novyny/sbu-ta-nato-posylyly-spivpratsiu-u-sferi-kiberbezpeky-vidbulasia-vzaiemna-intehratsiia-system-monitorynhu-zahroz>

<sup>178</sup> SSU, “Wives of Russian invaders call on their husbands to rape Ukrainian women (audio),”

況に引用されて、間違いなくロシア軍の評価を貶めた通信である。(2022年4月)(残虐性)

- ロシア兵士同士の(平文の)携帯電話での通信:民間人を殺せよと指示している内容。同時に、ウクライナ軍の兵員数を過大に見積もって怖がっている内容<sup>179</sup>。(2022年5月)(残虐性、厭戦気分)
- ロシア軍の契約兵士が妻と携帯電話で通話:将軍が大損害を被った部隊に前線への出撃を命じたが、兵士達が拒否して将軍に銃を向ける状態になったことを話した内容<sup>180</sup>。(2022年5月)(厭戦気分)
- ロシア軍兵士が故郷の父親とした電話通話:故郷に帰りたい兵士のために、同僚が指を砕いて除隊させた話。SSU 広報は、指を砕かなくても、ウクライナ軍に投降すれば良いと、電話のホットライン番号を掲示している<sup>181</sup>。(2022年6月)(投降勧告)
- ロシア兵士と故郷の親戚との電話通話:負傷したウクライナ兵を捕虜にせず、喉を掻き切った、戦友もそうしたと話す内容<sup>182</sup>。(2022年7月)(残虐性)

#### イ ロシアによる情報作戦への対抗

他方、ロシアは今次戦争でもサイバー空間において、偽情報を使用して広汎な情報作戦を展開している。その対象は、ロシア国民、ウクライナ国民、欧米諸国そして非同盟諸国にまで及んでいる<sup>183</sup>。これに対してSSUはロシアによる情報作戦を妨害阻止するために、通信傍受情報の公開に加えて、その検挙能力も活かして活動している。

- ロシアによる情報作戦の暴露:ロシア軍の「英雄」(ウクライナ兵20名以上を殺害して同僚を救ったとされた軍曹)が妻に電話で、自分一人が生き残っただけで、ウクライナ兵は殺害していないし同僚も救っていないと語り、ロシア軍による「英雄」創作を暴露<sup>184</sup>。(2022年6月)

---

*News*, 12 April 2022, accessed 1 June 2022, <https://ssu.gov.ua/en/novyny/wives-of-russian-invaders-call-on-their-husbands-to-rape-ukrainian-women-audio>

<sup>179</sup> SSU, “SSU interception: occupiers receive orders to shoot civilians (audio),” *News*, 5 April 2022, accessed 1 June 2022, <https://ssu.gov.ua/en/novyny/ssu-interception-occupiers-receive-orders-to-shoot-civilian>

<sup>180</sup> SSU, “Russian soldiers ready to kill generals who force them to go on offensive (audio),” *News*, 30 May 2022, accessed 1 June 2022, <https://ssu.gov.ua/en/novyny/russian-soldiers-ready-to-kill-generals-who-force-them-to-go-on-offensive-audio>

<sup>181</sup> SSU, “Occupiers continue to mutilate themselves to be declared unfit for war in Ukraine (audio),” *News*, 29 June 2022, accessed 30 June 2022, <https://ssu.gov.ua/en/novyny/rosiiski-okupanty-prodovzhuiut-kalichyty-sami-sebe-aby-yikh-vyznaly-neprydatnymi-dlia-viiny-v-ukraini-audio>

<sup>182</sup> SSU, “Occupiers brag to relatives how they finish off wounded Ukrainians (audio),” *News*, 2 July 2022, accessed 7 July 2022, <https://ssu.gov.ua/en/novyny/occupiers-brag-to-relatives-how-they-finish-off-wounded-ukrainians-audio>

<sup>183</sup> Microsoft, *ibid.*, pp.12-22.

<sup>184</sup> SSU, “SSU debunks russian fake about sergeant Krasnov whom propagandists try to picture as hero (video),” *News*, 27 June 2022, accessed 28 June 2022,

<https://ssu.gov.ua/en/novyny/sbu-rozvinchala-rosiiskiy-feik-pro-serzhanta-krasnova-yakoho-propahandysty-namahalysia-heroizuvaty-video>

- 情報作戦担当 FSB 作員（キーウ在住）を摘発：ウクライナで親ロシア感情を醸成するため、オンラインメディアを 20 作成して、ロシアの立場を正当化する虚偽情報を拡散（月間実アクセス者数 220 万人）していた<sup>185</sup>。（2022 年 6 月）
- 親ロシア情報拡散の阻止：2022 年 6 月の広報によれば、SSU はロシアの宣伝に対抗するために、親ロシアのユーチューブのチャンネル 500 近く（契約者 1500 万人）を閉鎖させ、他に、テレグラムのチャンネル 1529、インスタグラムのアカウント 426、フェイスブックのアカウント 93、ティックトックのアカウント 1050 の閉鎖を要請している<sup>186</sup>。
- SSU と軍情報部、共同声明を発表（2022 年 7 月 15 日）：国民に対して 100 のテレグラム・チャンネルを指定して、これらを見ないように呼び掛けた。これらのチャンネルは、一見独立系のように見えるが、実はロシアのインテリジェンス機関が資金援助と活動の調整をしている。偽情報や操作情報で溢れており、ロシアの対ウクライナ情報作戦に使用されている。SSU の今までの調査でそれが判明した。これらのチャンネルを支援する出版その他の活動は利敵行為となる。と注意を呼び掛けている<sup>187</sup>。
- 2022 年末の SSU サイバーセキュリティ部長のインタビューによれば、SSU は 2022 年中に、インターネット上で偽情報や親露情報を拡散して扇動者に対して 1200 の刑事手続きを開始し、600 人に対して犯罪容疑を通告し、230 人弱が拘禁刑の有罪判決を受けている。また、45 の大規模ボットファームを摘発阻止したが、これらのボットファームは 200 万以上の偽 SNS アカウントの容量があった<sup>188</sup>。

## （7）徴兵逃れの阻止・摘発

ロシア軍の侵攻に直面して、ウクライナ国民の多くは積極的に祖国防衛戦争に参加し或いは協力支援している。他方、人間は弱いものであり戦争から逃避したい者もいる。戦争への参加や協力は自由意志で自発的に行われるのが理想であろうが、現実はそうもいかない。国

<sup>185</sup> SSU, “SSU exposes russian agent who created 20 pro-russian online media in Ukraine (video),” *News*, 7 June 2022, accessed 10 June 2022, <https://ssu.gov.ua/en/novyny/sbu-vykryla-ahenta-rf-yakyi-stvoryv-20-prorosiiskiykh-internetzmi-v-ukraini-video>

<sup>186</sup> SSU, “SSU Cyber Department counters russian propaganda: almost 500 Youtube channels and several thousand accounts in social networks blocked (video),” *News*, 26 June 2022, accessed 28 June 2022, <https://ssu.gov.ua/en/novyny/kiberfakhivtsi-sbu-aktyvno-protydiut-rosiiskii-propahandi-zablokovano-maizhe-500-youtube-kanaliv-i-dekilka-tysiach-akauntiv-v-inshykh-sotsmerezhakh-video>

<sup>187</sup> SSU, “Joint statement on protection of Ukrainian information space from enemy Telegram channels,” *News*, 15 July 2022, accessed 16 July 2022, <https://ssu.gov.ua/en/novyny/spilna-zaiava-z-pryvodu-zakhystu-informatsiinoho-prostoru-ukrainy-vid-rosiiskiykh-vorozhykh-telehramkanaliv>

-- Defence Intelligence of the DoD of Ukraine, “Joint Statement Regarding the Countering the russian Aggression in Information Area of Ukraine,” 15 July 2022, accessed 16 July 2022, <https://gur.gov.ua/en/content/spilna-zayava-z-pryvodu-protydii-rosiyskiy-ahresiyi-v-informatsiynomu-poli-ukrayiny.html>

<sup>188</sup> SSU, “Since war started, SSU exposes over 1000 enemy Internet agitators spreading fakes about war in Ukraine – Illia Vitiuk,” *News*, 27 December 2022, accessed 3 January 2023, <https://ssu.gov.ua/en/novyny/sbu-vykryla-pid-chas-viiny-bilshe-1-tys-vorozhykh-internetahitoriv-yaki-poshyriuvaly-feiky-pro-viiny-v-ukraini-illia-vitiuk>

民の逃避を放置しては、更に多くの逃避者が生まれる可能性がある。そこでウクライナ政府はロシア軍の侵攻直後に徴兵対象である 18 歳から 60 歳の男子の徴兵逃れのための出国を禁止した。

ところが、いかにウクライナ国民全体の士気が高くても、中には徴兵を逃れるため、違法な出国を図る者もいる。そして金銭と引き換えに違法出国の支援をする者も尽きない。そこで SSU は、国境警備隊や国家捜査局 SBI、国家警察と協力して、徴兵逃れの違法出国支援者の取締りにも当たっている。違法出国支援の犯罪グループは、毎月コンスタントに数グループが摘発されている。

例えば、2022 年 10 月 1 ヶ月間を例にとると、7 件の検挙事例が広報されている。10 月 14 日の SSU 広報によれば、4 つのグループを摘発している。違法出国の方法は、身体障害者で兵役に適さないという偽造文書を作成して、これで国境検問所を通らせようとする者、或いは、国境警備の手薄なところから密出国を手引きする者などがいる。これらの事例では、1 人当たり 1700 米ドルから 7000 米ドルの報酬を得ていた<sup>189</sup>。また、10 月 24 日の SSU 広報によっても、2 つのグループの摘発が公表されている。これらの例では、人道支援物資の運搬者である旨の偽造文書を作成して、国境検問所を通過しようとする手口が暴露されている。報酬は 1 人当たり 1500 米ドルから 5500 米ドルである<sup>190</sup>。更に、10 月 27 日の SSU 広報によれば、地方検事局の次長が、徴兵逃れのため身体障害者登録を支援する報酬として 7500 ドルを受け取ったとして検挙拘束されている<sup>191</sup>。

徴兵逃れの基本的手法は三つである。先ず、国境検問所を通過するために出国を正当化する文書（兵役不適の証明書や人道物資の運搬者を証する文書）を偽装する手法、次に、国境の抜け道を案内する手法、更に、兵役不適の医者その他の権限ある者の文書を偽造する手法である。これらの手法による徴兵逃れを摘発して、阻止しようとしているのである。

## （8）まとめ

以上ウクライナ SSU の活動を見てきたが、その活動が極めて広範囲に及ぶことが明らかになった。ロシア工作員・協力者の摘発、ロシア侵攻軍に対する情報収集、サイバー攻撃対処、情報作戦とロシアの情報作戦への対抗などである。ロシア工作員・協力者の任務を見ても、単なる機密情報の収集にとどまらず、ロシア軍が攻撃に必要な標的情報の収集、侵略正

---

<sup>189</sup> SSU, “SSU shuts down another four channels used by draft evaders to illegally leave Ukraine,” *News*, 14 October 2022, accessed 16 October 2022, <https://ssu.gov.ua/en/novyny/sbu-likviduvala-shche-chotyry-kanaly-nelehalnoho-vyizdu-ukhyliantiv-yaki-ne-khotily-zakhyshchaty-ukrainu>

<sup>190</sup> SSU, “SSU shuts down new channels of draft evaders crossing border under cover of transporters of humanitarian aid,” *News*, 24 October 2022, accessed 27 October 2022, <https://ssu.gov.ua/en/novyny/sbu-likviduvala-novi-kanaly-vyizdu-ukhyliantiv-za-kordon-pid-vyhliadom-pereviznykiv-humanitarnoi-dopomohy>

<sup>191</sup> SSU, “SSU jointly with SBI detains high-ranking official of prosecutor’s office who ‘issued’ certificates of disability group for money,” *News*, 27 October 2022, accessed 1 November 2022, <https://ssu.gov.ua/en/novyny/sbu-spilno-z-dbr-zatrymala-vysokoposadovtsia-prokuratury-yakyi-za-hroshi-harantuvav-oformlennia-hrupy-invalidnosti>

当化や後方攪乱のためのテロ・破壊活動、更にはウクライナ世論に影響を与えるための情報工作など多彩である。もしSSUの諸活動がなければ、ウクライナは内部から崩壊した可能性もあった。国内を主たる対象とするセキュリティ・サービスの活動が戦争遂行では不可欠であることが良く理解できると考える。

このようなセキュリティ・サービスの基本的な情報収集手法・調査手法は、通信傍受、信書開披、監視機材（マイク、カメラ等）の設置、秘密搜索、潜入調査・囮調査などであり、尾行張込などという任意手段では到底その任務は全うできないのである。

他の民主主義国家にもセキュリティ・サービスは存在する。米国FBI、英国SS、フランスDGSI、ドイツBfVなどである。ウクライナSSU程の広汎な任務は兎に角として、最低限、敵性国家の工作員と協力者を摘発できなければ、戦う前に内部から崩壊してしまうのである。しかし、我が国には諸外国のセキュリティ・サービスと同様の機能を持つ組織は存在しない。

## 7 教訓：我が国インテリジェンス強化の方向性

以上、ロシア・ウクライナ戦争におけるウクライナのインテリジェンス優位を分析して来たが、背景には、第1に、米国を中心とするシギント、イミント、マシントなどの優れたインテリジェンス力があり、その米国がウクライナを支援していること、第2に、ウクライナ自身も優れたセキュリティ・サービスを保持していることが明らかになった。

この教訓に学べば、我が国におけるインテリジェンス強化の方向も自から明らかであろう。即ち第1に、我が国もシギント、イミント、マシントなどのインテリジェンス力を抜本的に強化する必要がある。しかし、日本が如何に努力しても、独力では米国並みどころか米国に近い水準に到達することも不可能である。今回のロシア・ウクライナ戦争でも、我が国よりも遥かに優れたインテリジェンス機関を擁するフランス・ドイツ両国とも、ロシアによる侵攻を予測できなかったのである。従って、米国と協力してインテリジェンス力を強化する他に道はない。UKUSAシギント同盟やASGイミント同盟への加盟も目指すべきである。我が国を取り巻く脅威を考えれば、我が国の安全保障のためには日米同盟以外の選択肢はあり得ず、軍事面に加えてインテリジェンス面でも強固な同盟関係を構築することが理に適っている。

ところで、軍事面でもインテリジェンス面でも、同盟の本質は、常にGive & Takeである。博愛事業ではないのである。こちらに提供できるものがなければ、受け取ることもできない。従って、インテリジェンスの分野でも米国と真の同盟関係に入るには、国家シギント機関、国家イミント機関、国防マシント機関を創設し或いは強化することが必要である。シギント、イミント、マシント分野で自助努力してこそ、米国との協力体制を強化できるのである。

第2に、インテリジェンスとしてのセキュリティ・サービスを整備することも必要である。ウクライナ戦争でウクライナ SSU が果たしている機能、特に敵国の作業者や協力者の摘発は戦時下の国家には必須のものであるが、我が国には現在その機能を十分に果たし得る機関が存在しない。国内インテリジェンスでも、国家が戦うことを想定した国家機関が存在しないのである。

以上を前提に、インテリジェンス強化のため方向性を提案したい<sup>192</sup>。先ず、インテリジェンス強化に当たっては、規模の違いはあれ、米国を手本とすべきである。米国のインテリジェンスは、その人員や予算規模が我が国とは比較にならない程巨大であって参考にならないと主張する者もいるが、手本にすべきはその人員や予算規模ではなく組織構成の仕方や運営である。筆者は、米国のインテリジェンス、特に NSA を研究してきたが、研究すればするほど、組織面でも機能面運用面でも米国インテリジェンスの合理性には感銘を受けざるを得ないのである（特に国家諜報長官による人事、予算、情報要求・配布における統括機能は、極めて重要である）。また、米国の組織制度を手本することにより、米国インテリジェンスとの協力関係の深化も容易となるであろう。

なお、英国インテリジェンスは、米国と比して規模が小さい割に極めて有能であるとして、我が国は英国インテリジェンスに倣うべきであると主張する者もいる。しかし、英国のインテリジェンス力には、米国との特殊関係、即ち UKUSA 同盟によるシグント力が大きく貢献しているのを忘れてはいけない。UKUSA シグント同盟がなければ、英国のインテリジェンス力も弱体となるのである。

以下の記述は、夢物語と映るかもしれないが、議論を始めなければ一歩も進むことはできないので、筆者が考える実現すべき理想像を記述する。

## （1）国家シグント機関の創設

### ア 組織任務

国家シグント機関を創設する。UKUSA 諸国がそうであるように、シグントのみならずサイバーセキュリティ担当の中核機関とする。そのため、平時から国家安全保障のための対外的なコンピューター網工作（CNE）を認める。また、インターネット通信の内、通信メタデータに対する傍受権限や我が国を経由する通過通信（外国間通信）に対する傍受権限など、シグント任務やサイバーセキュリティ任務を遂行するために必要な権限を整備する。有効なサイバーセキュリティ対策のためには、UKUSA 諸機関と協働する強力なシグント機関の設置が一番の近道である<sup>193</sup>。

### イ 人事

本部長及び副本部長は首相任免、部長級は官房長官任免とし、事前に内閣情報官の同意を必要とする。それ以下の人事は本部長の任免とする。専門性を確保するために、NSA に倣

<sup>192</sup> マシント機関については、専ら防衛省内の改革で情報本部において構築できるであろうから、ここでは言及を差し控える。

<sup>193</sup> 茂田忠良『サイバーセキュリティとシグント機関～NSA他UKUSA諸機関の取組』（情報セキュリティ総合科学、2019年11月）参照。



いシビリアン中心で独立した人事ができる組織とする。内閣情報調査室他、関係省庁との人事交流を進める。

#### ウ 予算

英国に倣い、人件費を含む予算は内閣官房にインテリジェンス関係予算として一括計上する。米国に倣い、予算立案は内閣情報官の権限とする。他の省庁予算とは別枠とする。

#### エ 運営

米国に倣い、任務付与・情報配布は、内閣情報官の権限とする。

#### オ 設置場所

防衛省に附置する。戦闘支援の必要を考慮すると米国 NSA に倣うべきである。但し、その任務は防衛省の所掌事務を超え、人事予算運営なども変則的であるので、国家行政組織法等の改正が必要であろう。

また、陸海空その他サービス・シグント組織を強化整備すると共に、米国の CSS（中央安全保障サービス）に倣い、統合調整機構も設置すべきである。

なお、防衛省に附置出来ない場合は、イタリアに倣い、情報省を創設して、その附置機関とすることも選択肢である。

## （２）国家イミント機関の創設

#### ア 組織任務

内閣衛星情報センターを抜本的に拡充して、国家イミント機関を創設する。米国 NGA に倣い、衛星情報のみならず、有人無人航空機による収集画像情報（自衛隊、海上保安庁、警察、消防が収集する情報も含む。）も統合分析する組織とする。また単なる画像分析から、米国 NGA のような高度な Geospatial-Intelligence 地理空間諜報への発展を目指すべきである。

#### イ 人事

現在の内閣衛星情報センターの大増員が不可欠である。現在の職員数は不明であるが、2011 年公表資料では 219 人であり併任者を加えても、実数は数百人であろう。現在の予算規模（年間約 800 億円）・収集アセットと比較して余りにも人員過少である。最低、千人以上の組織とする必要がある。

本部長及び副本部長は首相任免、部長級は官房長官任免とし、事前に内閣情報官の同意を必要とする。それ以下の人事は本部長の任免とする。専門性を確保するために、NGA に倣いシビリアン中心で独立した人事ができる組織とする。内閣情報調査室他、関係省庁との人事交流を進める。

#### ウ 予算

英国に倣い、人件費を含む予算は内閣官房にインテリジェンス関係予算として一括計上する。米国に倣い、予算立案は内閣情報官の権限とする。他の省庁予算とは別枠とする。

#### エ 運営

任務付与・情報配布は、内閣情報官の権限とする。

#### オ 設置場所

防衛省に附置する。但し、その任務は防衛省の所掌事務を超え、人事予算運営なども変則的であるので、国家行政組織法等の改正が必要であろう。

なお、防衛省に附置出来ない場合は、イタリアに倣い、情報省を創設して、その附置機関とすることも選択肢である。

### (3) セキュリティ・サービスの創設

現在、セキュリティ・サービス機能は警察の警備部門が担っているが、現在の権限・運営では全く不十分な機能しか発揮していないのは明白である<sup>194</sup>。平時の外国の工作人員や協力者の摘発自体が全く不十分なのが現状である。ロシア・ウクライナ戦争を見れば、戦時においては敵国の工作人員や協力者を迅速に摘発する必要性は極めて高いが、我が国にはそのような権能を発揮できる機関は存在しない。

FBIには国家安全保障に関する調査を行う国家安全保障局がある。これに倣って、国家安全保障のための調査活動を主任務とする組織を設置して、これに、FBI国家安全保障局と同様に、通信傍受、秘密搜索、監視機材の設置、囮・潜入調査などの権限を付与して、情報収集力を欧米並みに強化する必要がある。

このような任務権限を付与する組織としては、既存の組織では、過去のスパイ摘発の実績を見ても先ず警視庁公安部が適切であろう。公安調査庁も選択肢であるが、オウム真理教事件で解散指定することが出来なかったことから見ても情報収集力は弱体である。また、公安調査庁の情報からスパイ検挙に至った事例など寡聞にして聞いたことがない。公安調査庁は不適切であろう。

なお、国家安全保障のために通信傍受、秘密搜索などを行うため、米国の対外諜報監視裁判所（FISC）と同様な組織を設置して許可令状を発布する制度を構築する必要があるだろう。

---

<sup>194</sup> 詳しくは、茂田忠良『テロ対策に見る我が国の課題』（警察政策学会資料第113号、2021年11月）参照。

警察政策学会資料 第125号の再訂版

ウクライナ戦争の教訓  
～我が国インテリジェンス強化の方向性～  
(再訂版)

令和4(2022)年 9月 初版発行

令和4(2022)年 12月 改訂版発行

令和5(2022)年 7月 再訂版発行