

# 国立国会図書館 調査及び立法考査局

Research and Legislative Reference Bureau  
National Diet Library

論題 Title	ロシアによるウクライナ侵略をめぐる「情報戦」
他言語論題 Title in other language	Information Warfare and Russian Aggression against Ukraine
著者 / 所属 Author(s)	青井佳恵 (AOI Yoshie) / 外交防衛課
書名 Title of Book	ロシアによるウクライナ侵略をめぐる諸問題 : 総合調査報告書
シリーズ Series	調査資料 2023-3 (Research Materials 2023-3)
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
刊行日 Issue Date	2024-3-14
ページ Pages	41-57
ISBN	978-4-87582-921-8
本文の言語 Language	日本語 (Japanese)
摘要 Abstract	ロシアによるウクライナ侵略に際し展開されてきたサイバー攻撃、偽情報の流布、ナラティブの戦い、通信インフラの確保、開示による抑止といった現代社会における情報戦の影響と対応を紹介する。

\* この記事は、調査及び立法考査局内において、国政審議に係る有用性、記述の中立性、客観性及び正確性、論旨の明晰（めいせき）性等の観点からの審査を経たものです。

\* 本文中の意見にわたる部分は、筆者の個人的見解です。

# ロシアによるウクライナ侵略をめぐる「情報戦」

国立国会図書館 調査及び立法考査局  
外交防衛課 青井 佳恵

## 目 次

はじめに

### I 情報戦とは

- 1 首相、閣僚等による国会答弁及び防衛省による説明
- 2 有識者、専門書等による説明

### II ロシアによるウクライナ侵略において実施された情報戦の事例

- 1 ロシアによる情報戦
- 2 ウクライナによる情報戦
- 3 ロシア及びウクライナ以外の主体の動向

おわりに

キーワード：ロシアによるウクライナ侵略、情報戦、サイバー攻撃、認知戦、影響工作、  
偽情報、デイスインフォメーション、ナラティブ、開示による抑止

## はじめに

2022年2月にロシアによるウクライナ侵略が開始される前後から、「情報戦」という用語が報道記事等にしばしば登場するようになった。「情報戦」は目新しい概念ではないが、「情報戦」に何が含まれるのか明示される機会は稀であり、意味するところが曖昧なまま、漠然としたイメージが独り歩きしている。例えば、侵攻開始の直後に読売新聞が「ロシアとウクライナによる情報戦の主な例」をまとめた記事において、ロシアについては「対外向けテレビ放送を通じ、真偽不明のウクライナに関する情報を放送」、「ウクライナ地方行政のサイトへのサイバー攻撃」、「国営テレビで、ウクライナの偽情報への注意を呼びかけ」が、ウクライナについては「国連大使が、死亡したロシア兵が残したメッセージを読み上げ」、「ロシア兵捕虜の映像をSNS上で公開」が挙げられている<sup>(1)</sup>。ほかにも、ファクトチェック団体等による情報の精査（後述II-1(3)及び3(2))、ウクライナ政府の呼びかけによりボランティアが連帯した「IT軍」の活動（後述II-2(2))、米国政府等によるインテリジェンス（機密情報）の公開（後述II-3(1)）に、「情報戦」の文脈で言及した記事が見受けられる<sup>(2)</sup>。

本稿では、Iにおいて「情報戦」についての首相、閣僚等による国会答弁及び防衛省による説明並びに有識者、専門書等による説明を紹介する。IIにおいて、ロシアがウクライナへの侵略を準備し、2022年2月に大規模な軍事侵攻を開始した過程で、ロシア、ウクライナ等がどのような「情報戦」を展開してきたのか、事例を紹介する。なお、以下本稿では「情報戦」について括弧を付さずに表記する。

## I 情報戦とは

## 1 首相、閣僚等による国会答弁及び防衛省による説明

まず、情報戦に関する近年の首相、閣僚等による主な国会答弁を紹介する。岸田文雄内閣総理大臣は、2022（令和4）年5月26日の衆議院予算委員会において、ウクライナ情勢を踏まえて、フェイクニュース及びソーシャル・ネットワーキング・サービス（SNS）による偽情報による認知戦<sup>(3)</sup>への対応、認知領域を含む情報戦への対応が重要であるとの認識を示している<sup>(4)</sup>。林芳正外務大臣（当時）は、2023（令和5）年3月10日の衆議院外務委員会において、「インテリジェンスにおける公開情報の活用、これは情報戦への対応の観点からも極めて重要だ」との認識を示している<sup>(5)</sup>。より具体的な対策等への言及として、田部井貞明防衛省大臣官房審議官（当時）は、国際社会において有事に至る前の段階から、偽情報の流布により他国の意思決定に影響を及ぼすと

\* 本稿は、令和6（2024）年1月5日時点までの情報を基にしている。インターネット情報への最終アクセス日も同日である。

(1) 「露・ウクライナ 情報戦 SNSなど拡散」『読売新聞』2022.3.8.

(2) 「「虚偽」情報・砲弾飛び交う ウクライナ東部 米「ロシアの口実作り本格化」 機密の事前開示で対抗」『朝日新聞』2022.2.20.

(3) 認知戦とは、ターゲットとなる国民、組織、国家に干渉する又は国家を不安定化させることを目的とし、ターゲットの考え方や選択に影響を与え、意思決定の自律性を弱体化させるために用いられる作戦である（栗原響子「外交と偽情報—ディスイنفォメーションという脅威—」小泉悠ほか『偽情報戦争—あなたの頭の中で起こる戦い—』ウェッジ, 2023, p.24.）。

(4) 第208回国会衆議院予算委員会議録第19号 令和4年5月26日 p.6.

(5) 第211回国会衆議院外務委員会議録第2号 令和5年3月10日 p.6.

いった情報戦に重点が置かれている旨を指摘し、日本においても認知領域を含む情報戦への対応として、人工知能/AIを活用した分析機能の整備を行い、偽情報の見破りや分析、迅速かつ適切な情報発信等に取り組む考えを示している(2023(令和5)年3月29日 衆議院内閣委員会)<sup>(6)</sup>。岡野結城子外務省大臣官房政策立案参事官(当時)は、情報の収集・分析の強化とともに、その結果を踏まえて日本として発信すべきナラティブ(後述II-1(4))の迅速な構築及び発信を行っていくことの重要性を指摘している(2023(令和5)年4月10日 参議院決算委員会)<sup>(7)</sup>。ただし、近年の国会答弁等において、日本政府による情報戦の定義は明確に示されてこなかった。

2022(令和4)年12月に閣議決定された安全保障三文書において情報戦という用語が用いられており<sup>(8)</sup>、2023(令和5)年7月に刊行された防衛白書(令和5年版)において、防衛省による情報戦の定義が初めて示された。同書に、情報戦とは、「紛争が生起していない段階から、偽情報や戦略的な情報発信などを用いて他国の世論・意思決定に影響を及ぼすとともに、自らの意思決定への影響を局限することで、自らに有利な安全保障環境の構築を企図すること」であり、国際社会において情報戦に重点が置かれている旨が述べられている<sup>(9)</sup>。「ロシアによるウクライナ侵略の状況を踏まえれば、わが国防衛の観点から、偽情報の見破りや分析、そして迅速かつ適切な情報発信などを肝とした認知領域を含む情報戦への対応が急務である」と述べられる一方、防衛省及び自衛隊の取組として、SNSなどを介した偽情報の流布、世論操作、謀略などは日本の信頼を毀損するとして実施しない旨が明言されている<sup>(10)</sup>。

## 2 有識者、専門書等による説明

大澤淳氏(中曽根康弘世界平和研究所主任研究員)は、情報戦を「相手国に対して偽情報(ディスインフォメーション)を流し、政治体制や指導者に対する国民の信頼を失墜させ、社会を不安定化する行為や、自国民を団結させるプロパガンダ、国際社会に対して支持を取り付ける世論戦など、情報操作を用いて自国に有利な状況をつくる影響力工作のこと」と説明する<sup>(11)</sup>。また、『インテリジェンス用語事典』によれば、「情報戦(Information Warfare: IW)」は、「味方の情報および情報システムを防護し、かつ敵のそれを攻撃・攪乱・妨害する敵味方相互の情報活動。基本的な概念は、情報が必要な時に必要な人へ、必要な内容で伝えられることをめぐる戦いの一局面」である<sup>(12)</sup>。

(6) 第211回国会衆議院内閣委員会議録第9号 令和5年3月29日 p.21.

(7) 第211回国会参議院決算委員会議録第4号 令和5年4月10日 p.28.

(8) 「国家安全保障戦略」(令和4年12月16日国家安全保障会議決定・閣議決定) pp.4, 7. 内閣官房ウェブサイト <<https://www.cas.go.jp/jp/siryoku/221216anzenhoshounss-j.pdf>>; 「国家防衛戦略」(令和4年12月16日国家安全保障会議決定・閣議決定) pp.2, 8, 11. 防衛省ウェブサイト <<https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy.pdf>>; 「防衛装備計画」(令和4年12月16日国家安全保障会議決定・閣議決定) p.8. 同 <<https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/plan.pdf>>

(9) 防衛省『日本の防衛—防衛白書— 令和5年版』日経印刷, 2023, p.167.

(10) 同上, p.309.

(11) 大澤淳ほか「座談会 戦場はスマホの中に—「ナラティブ」が情報戦の最前線—」『外交』80号, 2023.7・8, p.11. プロパガンダの目的は、人々の考え方に影響を与えるのではなく、人々を特定の思想に誘導し態度や行動に影響を与えることである(栗原 前掲注(3), p.26.)。

(12) 川上高司監修, 樋口敬祐ほか『インテリジェンス用語事典』並木書房, 2022, p.224. なお、一般的な用語辞典では、『イミダス 2006』に、元防衛研究所主任研究員である中村好寿氏が、「情報戦(Information Warfare: IW)」について、「敵よりも優位に立つため、敵の情報活動(収集・処理・評価・伝達)、情報システム(情報要員・部隊、情報組織、情報機材)、保有する情報内容に影響を及ぼすとともにわが方への影響を阻止・妨害する戦い。具体的形態として①諜報戦(収集活動と保全)、②指揮・統制戦(指揮・統制システムの破壊、切断と防護)、③電子戦(電磁波の利用と阻止・妨害)、④心理・宣伝戦(心理・宣伝活動と阻止・妨害)、⑤サイバー戦(サイバー空間の利用と阻止・妨害)等がある」との説明を寄せている(中村好寿「国際関係—軍事—情報戦(IW)」『イミダス 2006』集英社, 2006, p.548.)。

ローレンス・フリードマン (Lawrence Freedman) 氏 (ロンドン大学キングスカレッジ名誉教授) は、情報戦には2つの混同しやすい意味——1つは情報が流れるシステムそのものを無効にするための手段 (工学的なもの)、もう1つは情報の内容に影響を与えることで認識に影響を及ぼそうとする試み (人間の認識に関するもの) ——が込められていると説明する<sup>(13)</sup>。

ロシアによるウクライナ侵略に引き付けると、元在ロシア日本国大使館防衛駐在官の佐々木孝博氏 (広島大学客員教授) は、ロシアの戦略文書に基づいて、情報戦を「単に技術的な情報セキュリティのみならず、広く、情報空間を使った政治的、経済的、社会的システムを狙った戦いと捉え、それによって国家の意思決定者の心理的操作を含む「認知領域の戦い (認知戦)」とも捉えている」と分析する<sup>(14)</sup>。なお、米国政府による情報戦 (IW) の公式な定義がないことは、複数の研究者が指摘している<sup>(15)</sup>。

また、佐々木氏は、情報戦に関する取組を個別に挙げるのではなく、構造的な整理を試みて、情報戦を2種類に大別する分類を示している。第一は、平時・有事問わず行われる、国家の施策に影響を及ぼすために行う活動や国家指導者や軍事指導者の意思決定に影響を及ぼす活動、国民の世論を誘導するために行う活動などの「戦略的な情報戦」であり、第二は、紛争・戦争など有事に至った場合に、軍事力をいかに運用するかの作戦・戦術の見地で、敵の状況を把握したり、自らの行動を欺瞞 (ぎまん) したりする目的で行う「作戦・戦術的な情報戦」である<sup>(16)</sup>。

さらに別の整理として、青井千由紀氏 (東京大学教授) は、情報戦を「構築的」と「妨害的」の2種類に分類し、前者を「ナラティブを行使し、情報と行動とを相乗的に組み合わせ、受け手の認識を操作すること」、後者を「妨害工作」で、「相手を混乱させるようなディスインフォメーション (偽情報) の流布」などであるとする<sup>(17)</sup>。

## II ロシアによるウクライナ侵略において実施された情報戦の事例

IIでは、近年及び2022年2月にロシアによるウクライナへの大規模な軍事侵攻が開始された過程で、報道記事等において情報戦として扱われてきた事例を紹介する。

また、事例の紹介に先立って、Iで紹介したことを踏まえて情報戦及びロシアによるウクライナ侵略におけるその事例をイメージで表現した (図)。

(13) ローレンス・フリードマン (奥山真司訳) 『戦争の未来—人類はいつも「次の戦争」を予測する—』中央公論新社, 2021, pp.350-351. (原書名: Lawrence Freedman, *The future of war: a history*, London: Allen Lane, 2017.)

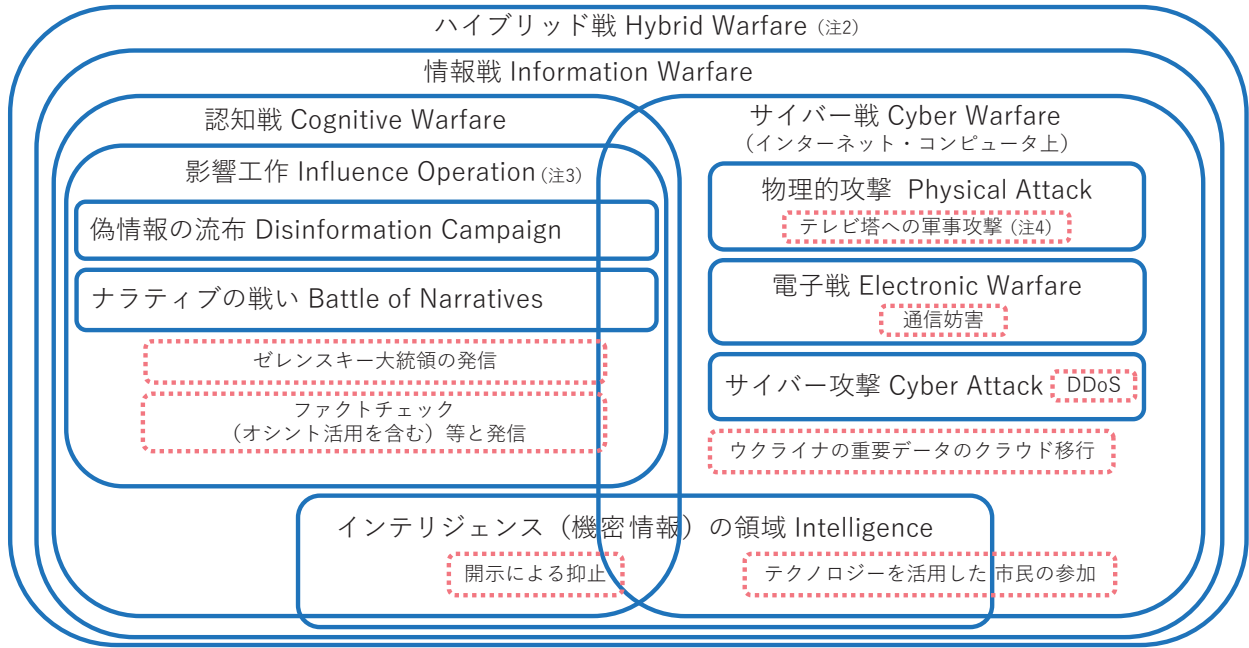
(14) 渡部悦和ほか『プーチンの「超限戦」—その全貌と失敗の本質—』ワニ・プラス, 2022, p.164. ロシアの情報戦については、ジャイルズ (Keir Giles) 氏 (英王立国際問題研究所上級研究員) がNATO国防大学のプロジェクトの一環としてまとめた資料に詳しい (Keir Giles, *Handbook of Russian Information Warfare*, Roma: NATO Defense College, November 2016, p.4. <<https://www.ndc.nato.int/download/downloads.php?icode=506>>). なお、2011年に制定されロシア国防省ウェブサイトにおいて公開されている「情報空間 (サイバー空間) におけるロシア軍の活動に関するコンセプト」において、情報戦 (サイバー戦) は、「情報システム、情報プロセス及び情報資源、その他の重要インフラを破壊させるための、情報空間 (サイバー空間) における2ないしそれ以上の国家間の争い」と定義されている (佐々木孝博「ロシアのサイバー戦略—「サイバー戦コンセプト」を中心に—」『日本大学大学院総合社会情報研究科紀要』13号, 2012, p.7.). 佐々木氏は、ロシアのプーチン (Vladimir Vladimirovich Putin) 大統領が2012年に発表した論文「強くあれ—ロシアの国家安全保障—」において、「情報空間」と「サイバー空間」がほぼ同義語として使用されていることを指摘する (同, p.1.).

(15) 渡部悦和「米国の情報戦」『東亜』658号, 2022.4, p.76; Catherine A. Theohary, “Defense Primer: Information Operations,” *In Focus*, IF10771, Updated December 14, 2023. <<https://crsreports.congress.gov/product/pdf/IF/IF10771>>

(16) 佐々木孝博「ロシア情報戦は「認知領域」を標的に」『外交』80号, 2023.7・8, pp.22-27.

(17) 「情報戦、戦略的発信で効果 東大教授 青井千由紀氏」『日本経済新聞』2021.9.25; 青井千由紀『戦略的コミュニケーションと国際政治—新しい安全保障政策の論理—』日経BP日本経済新聞出版, 2022, pp.159-164.

図 情報戦及びロシアによるウクライナ侵略におけるその事例のイメージ



(注1) 実線で囲った部分は概念レベルの用語であり、点線で囲った部分は具体的な出来事やツールを用いた行動などである。本稿の本文において言及がない用語を中心に注を付した。

(注2) 防衛白書において、「いわゆる「ハイブリッド戦」は、軍事と非軍事の境界を意図的に曖昧にした手法であり、このような手法は、相手方に軍事面にとどまらない複雑な対応を強いる」ことになる、「例えば、国籍を隠した不明部隊を用いた作戦、サイバー攻撃による通信・重要インフラの妨害、インターネットやメディアを通じた偽情報の流布などによる影響工作を複合的に用いた手法が、「ハイブリッド戦」に該当する」と考えている、と述べられている（防衛省『日本の防衛—防衛白書— 令和5年版』日経印刷, 2023, p.33.）。「2014年のロシアによるクリミア併合やウクライナ東部への軍事介入以降、その「ロシアとウクライナの間の」戦争こそがハイブリッド戦争と認識されるようになった」（〔 〕内は筆者による補記）とされる（川上高司監修、樋口敬祐ほか『インテリジェンス用語事典』並木書房, 2022, pp.319-320.）。各国ごとにハイブリッド戦争の捉え方は様々であり、統一された定義はないとされる（同）。ハイブリッド戦争（Hybrid War）とハイブリッド戦（Hybrid Warfare）については、戦略レベルから具体的な手法まで様々なレベルの議論があり十分に整理されているとは言えない。

(注3) 影響工作とは、平時から有事、そして紛争後に、相手国世論の意見や態度を自らの国益と目的を促進させる方向に醸成するため、外交、軍事、経済、サイバー、情報、その他の能力を統合・連携させ適用することである（栗原響子「外交と偽情報—ディスインフォメーションという脅威—」小泉悠ほか『偽情報戦争—あなたの頭の中で起こる戦い—』ウェッジ, 2023, p.24.）。本図では、ロシアとウクライナの双方による動きを影響工作の範囲に含めている。なお、影響工作に対する通信・インターネット企業等の役割に言及した論文、久古聡美「デジタル影響工作をめぐる動向と対応」が、当館刊行物『デジタル時代の技術と社会』（科学技術に関する調査プロジェクト2023報告書）（2024年3月刊行予定）に収録される。

(注4) 2022年3月1日、ロシア国防省は、ウクライナとの情報戦に対処するとしてキーウ中心部にある情報関連の軍特殊機関等への攻撃を警告して住民に退去を呼びかけており、同日、キーウのテレビ塔がロシアのロケット弾の攻撃を受けた（「露、キエフ通信網攻撃 TV塔にミサイル 5人死亡」『読売新聞』2022.3.2, 夕刊.）。

(出典) 下記の文献を参考に筆者作成。

長迫智子「「情報戦は地政学」ロシアの偽情報戦略を解く」『外交』73号, 2022.5・6, p.60; 渡部悦和ほか『プーチンの「超限戦」—その全貌と失敗の本質—』ワニ・プラス, 2022, p.196; 栗原響子「「人間の認知」をめぐる介入戦略—複雑化する領域と手段、戦略的コミュニケーション強化のための一考察—」『Roles Report』12号, p.8. <<https://roles.rcast.u-tokyo.ac.jp/uploads/publication/file/19/publication.pdf>>; 同「外交と偽情報—ディスインフォメーションという脅威—」小泉悠ほか『偽情報戦争—あなたの頭の中で起こる戦い—』ウェッジ, 2023, p.26; 飯塚恵子『ドキュメント誘導工作—情報操作の巧妙な罠—』中央公論新社, 2019, p.66; 齋藤孝道「情報戦における世論誘導工作の片鱗—サイバーインフルエンスオペレーションと国内での概況—」『防衛技術ジャーナル』43巻1号, 2023.1, p.7; Tzu-Chieh Hung and Tzu-Wei Hung, “How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars,” *Journal of Global Security Studies*, vol.7 Iss.4, December 2022, p.3. <<https://academic.oup.com/jogss/article-pdf/7/4/ogac016/45032748/ogac016.pdf>>; 志田淳二郎「ハイブリッド戦争とは何か(2)ロシアによる独自解釈」『治安フォーラム』29巻6号, 2023.6, pp.48-50; 田中達浩ほか「兵器なき戦場—としてのサイバー空間」『Voice』536号, 2022.8, p.187; 廣瀬陽子『ハイブリッド戦争—ロシアの新しい国家戦略—』講談社, 2021, pp.143-145; 大澤淳「ウクライナにおけるハイブリッド戦の様相と日本の防衛力強化への示唆」2022.9.6, pp.2, 11. 財務省ウェブサイト <<https://www.mof.go.jp/pri/research/seminar/fy2022/lm20220906.pdf>>; 佐藤雅俊、上田篤盛『情報戦、心理戦、そして認知戦—サイバーセキュリティを強化する—』並木書房, 2023, pp.9-10.

## 1 ロシアによる情報戦

### (1) サイバー攻撃

サイバー攻撃（cyber attack）とは、個人及び企業、政府機関等の組織を対象に、ネットワークを通じて行われる攻撃や破壊活動である<sup>(18)</sup>。ウクライナ国家特殊通信・情報保護局の関係者は、ウクライナに対するロシアのサイバー攻撃が始まったのは2022年1月14日だったと述べている<sup>(19)</sup>。同日、ウクライナ内閣、国防省を含む政府機関の約70の公式サイトがサイバー攻撃を受け、そのうち22の省庁のウェブサイトが改ざんされて、ウクライナ人の個人情報や全てネットワーク上に公開された等とする脅迫メッセージが表示される現象が発生した<sup>(20)</sup>。ワイパー（相手のシステム内のデータを消し、業務継続できなくすることを狙ったコンピュータウイルス）の大規模な被害を受けたウェブサイトも6つあった<sup>(21)</sup>。ウクライナ保安庁は同日、ウェブサイト上に、ほとんどのウェブサイトが復旧済みであり個人情報も盗まれていなかった旨を公表した<sup>(22)</sup>。ウクライナ側は後に、復旧に1週間かかったウェブサイトがあったもののデータは失われておらず、市民をパニックに陥れようとする心理戦であったと説明した<sup>(23)</sup>。

2月15日には、ウクライナの国防省及び2つの国営銀行のオシチャド（Oschad）とプライベート（Privat）のウェブサイトにDDoS攻撃（大量のデータを送り付けてサーバーに負担を与えて妨害する攻撃）が行われた<sup>(24)</sup>。銀行のシステム障害は一時的だったが、攻撃者は銀行の顧客宛に「銀行のATMが機能していない」という偽のテキストメッセージを流布し、ウクライナ市民の混乱につながった<sup>(25)</sup>。米国及び英国政府は、ロシア連邦軍参謀本部情報総局（GRU）がこの攻撃に関与していると明言している<sup>(26)</sup>。翌16日、ウクライナのフェードロフ（Mykhailo Fedorov）副首相兼デジタル化担当相は、これらの攻撃の主な目的は、ウクライナ市民を不安に陥れ、パニックを引き起こし、混乱させることであると述べた<sup>(27)</sup>。

また、同月23日には、GRUにより、ウクライナ政府及びIT、エネルギー、金融などの重要

(18) 「サイバー攻撃とサイバーセキュリティについてわかりやすく解説します」カスペルスキーウェブサイト <<https://www.kaspersky.co.jp/resource-center/definitions/what-is-cyber-security>>

(19) 「“見えない戦い”―現地取材で見てきた「ハイブリッド戦」の実態―」2022.7.27. NHK ウェブサイト <[https://www3.nhk.or.jp/news/special/sci\\_cul/2022/07/special/cyber-ukraine-0728/](https://www3.nhk.or.jp/news/special/sci_cul/2022/07/special/cyber-ukraine-0728/)>; 「ロシアのサイバー攻撃 被害限定的」『朝日新聞』2022.7.30.

(20) 「“見えない戦い”」同上; Jakub Przetacznik and Simona Tarpova, “Russia’s war on Ukraine: Timeline of cyber-attacks,” PE733.549, June 2022, p.3. European Parliament website <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS\\_BRI\(2022\)733549\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf)>; 松原実穂子『ウクライナのサイバー戦争』新潮社, 2023, pp.39-40.

(21) 松原 同上, pp.25, 39.

(22) 同上, p.40.

(23) 「ロシアからのハッキングに対抗するウクライナ、その“サイバー戦争”の指揮官の勝算」2022.9.22. Wired ウェブサイト <<https://wired.jp/article/yurii-shchyhol-urkraine-cyberwar-russia/>>; ゴードン・コレラ「ドローンからハッキングまで……ウクライナの前線で繰り広げられるハイテク戦争」2023.9.8. BBC website <<https://www.bbc.com/japanese/features-and-analysis-66725693>>

(24) 川口貴久「ウクライナ全面侵攻で高まる全世界のサイバーリスク」2022.3.2. Wedge Online ウェブサイト <<https://wedge.ismedia.jp/articles/-/25913>>

(25) 同上; 「ロシア、サイバー多重攻撃 サイト障害や偽メッセージ 周到準備、社会かく乱」『日本経済新聞』2022.2.27.

(26) Steve Holland and James Person, “US, UK: Russia responsible for cyberattack against Ukrainian banks,” *Reuters*, February 19, 2022. <<https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/>>; “UK assesses Russian involvement in cyber attacks on Ukraine,” 18 February 2022. Gov.uk website <<https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine>>

(27) Valerie Hopkins, “A hack of the Defense Ministry, army and state banks was the largest of its kind in Ukraine’s history,” *New York Times*, February 15, 2022. ロシア側は関与を否定している (*ibid.*)。なお出典記事は、2022年2月16日のウクライナで行われたフェードロフ氏の会見を、時差の関係で同月15日に報じている。

な民間インフラへのサイバー攻撃が行われ、多数のコンピュータにデータ消去プログラムがインストールされた<sup>28)</sup>。侵略が開始された2月24日以降には、米衛星通信大手ヴィアサット社が管理する通信衛星「KA-SAT」や、ウクライナからルーマニアに入るための国境検問所のコンピュータがサイバー攻撃の被害を受けるなど、攻撃は続けられていた<sup>29)</sup>。

## (2) 偽旗作戦

偽旗作戦 (false-flag operation) とは、「相手を非難したり自国の正当性を高めたりする目的で、自身が政治的・軍事的攻撃を受けているように演出する作戦」である<sup>30)</sup>。軍事侵攻開始前には、ロシアによる偽旗作戦が行われる懸念が示されていた。2022年1月から2月にかけて、米国政府は機密情報に基づいて、ウクライナ東部においてロシアが偽旗作戦を行うための工作員——市街戦の訓練やロシアの代理部隊に対する爆発物を用いた妨害行為を行う訓練を受けている——が既に配置されていること、偽の爆発、死体と弔問者を演じる者、破壊された場所や軍事装備などをロシアの諜報機関が捏造 (ねつぞう) して作成したプロパガンダ映像の公表をロシア側が検討していることなどを公表した<sup>31)</sup>。ブリンケン (Antony Blinken) 米 국무長官は、2022年2月17日の国連安全保障理事会において、ロシアが攻撃の口実作りを行っている旨を述べ、具体的な事柄として、ロシア国内におけるテロリストによる爆破事件の捏造、民間人に対するドローン攻撃の演出、化学兵器による攻撃の偽装等を挙げた<sup>32)</sup>。

## (3) ディスインフォメーション・キャンペーン—偽情報の流布—

偽情報 (disinformation. ディスインフォメーション) とは、「政治的・経済的利益を得ること、または意図的に大衆を欺くことを目的として作成された虚偽または誤解を招く情報」であり、近年のソーシャルメディアの普及によって、拡散される速度は速く、範囲は広がっている<sup>33)</sup>。偽情報と次項で紹介するナラティブの事例を明確に分類するのは難しいが、本稿では、ファクトチェックにより対応可能な事例を前者、真偽の確認を行うだけではうまく対抗できない事例を後者として挙げた。

ウクライナ情勢をめぐる、次に紹介するとおり1つの事柄に対してロシア政府及び露メ

28) “Ukraine computers hit by data-wiping software as Russia launched invasion,” *Reuters*, February 25, 2022. <<https://www.reuters.com/world/europe/ukrainian-government-foreign-ministry-parliament-websites-down-2022-02-23/>>; Matthias Schulze and Mika Kerttunen, “Cyber Operations in Russia’s War against Ukraine,” *SWP Comment*, No.23, April 2023, p.5. <[https://www.swp-berlin.org/publications/products/comments/2023C23\\_CyberOperations\\_UkraineWar.pdf](https://www.swp-berlin.org/publications/products/comments/2023C23_CyberOperations_UkraineWar.pdf)>

29) 松原 前掲注(20), pp.56-62.

30) 本山功「危機交渉における「弱さを偽る」戦略(下) —明確な脅しを欠いたロシアによる危機交渉の戦略的論理—」『NIDS コメンタリー』285号, 2023.11.14, p.7. <<https://www.nids.mod.go.jp/publication/commentary/pdf/commentary285.pdf>>; なお偽旗という用語は、中世において海賊船が、友好国又は中立国を示す偽の旗を掲げて獲物とする商船をおびき寄せていたことに由来する (“False flags: What are they and when have they been used?” *BBC*, 18 February 2022. <<https://www.bbc.com/news/world-60434579>>; Peter R. Mansoor, “False-Flag Operations,” February 23, 2022. Hoover Institution website <<https://www.hoover.org/research/false-flag-operations>>).

31) “Press Briefing by Press Secretary Jen Psaki and FEMA Administrator Deanne Criswell, January 14, 2022,” January 14, 2022. White House website <<https://www.whitehouse.gov/briefing-room/press-briefings/2022/01/14/press-briefing-by-press-secretary-jen-psaki-and-fema-administrator-deanne-criswell-january-14-2022/>>; “Department Press Briefing – February 3, 2022,” February 3, 2022. U.S. Department of State website <<https://www.state.gov/briefings/department-press-briefing-february-3-2022/>>

32) UN doc. S/PV.8968, 17 February 2022, p.12. <<https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=S/PV.8968&Lang=E>>

33) 栗原 前掲注(3), p.19.



ディアとウクライナ政府及びウクライナ・米欧メディアとの間で異なる見解が述べられている事例が見られる。

キーウ近郊のブチャにおいては、2022年3月30日頃にロシア軍が撤退した後、4月初旬に路上に多数の民間人の遺体が放置されているのが西側メディアに報じられ、大きな注目を集めた<sup>34)</sup>。手を縛られた遺体、後頭部に銃撃を受けた遺体、殺害前にレイプされた傷跡がある遺体もあった<sup>35)</sup>。これに対して、「3月30日にロシア軍が撤退した後に死亡したことは明らかである」、「ナチスは路上にいる人々を武装しているか否かにかかわらず殺害した」、「拡散されている動画の道路に横たわる「遺体」は移動しており、西側メディア等により演出された映像である」といった情報が拡散されたが、EUvsDisinfo（後述II-3(2)）により偽情報と判断されている<sup>36)</sup>。なお、ブチャにおける虐殺については、ガルージン（Mikhail Galuzin）駐日ロシア大使（当時）も、ロシア軍が撤退した後、最初にブチャに入ったのはウクライナの特務機関であり、「遺体を持ってきて、ロシア軍の犯罪に仕立て上げた」、「ブチャなどでロシア軍が行った虐殺の事実は一切ありません」と述べていた<sup>37)</sup>。

情報の真偽が明らかでないまま、両国の政権による「事実」の発表の応酬が展開された事例として、2022年3月のマリウポリの産院への爆撃が挙げられる。3月9日、ゼレンスキー（Volodymyr Zelenskyy）大統領は自らのツイッター（当時）に、マリウポリの産院が爆撃されたことを動画付きで投稿した<sup>38)</sup>。翌10日、ロシアのラブロフ（Sergey Lavrov）外相は記者会見の場で、「その産科病院ははるか以前に過激派に占領され、妊婦や看護職員らが追い出されていた」と述べた<sup>39)</sup>。さらに同日、在英ロシア大使館は、産院から救助されたとされる女性はモデルであると主張した<sup>40)</sup>。ロシア側から「モデル」とされた女性は、後日受けたインタビューで、攻撃を受けた当時、病院において治療が行われていた旨を述べており<sup>41)</sup>、また、EUvsDisinfoは、妊婦であったその女性が無事に出産したこと等を確認している<sup>42)</sup>。

なお、EUvsDisinfo 以外にロシア・ウクライナ情勢に関してファクトチェックが行われている

34) Malachy Browne et al., “Satellite images show bodies lay in Bucha for weeks, despite Russian claims,” *New York Times*, April 4, 2022.

35) *ibid.*; Lorenzo Tondo and Isobel Koshiw, “Evidence some Ukrainian women raped before being killed, say doctors,” *Guardian*, 25 April 2022. <<https://www.theguardian.com/world/2022/apr/25/evidence-ukraine-women-raped-before-being-killed-say-doctors-russia-war>>

36) “Disinfo: Those Failed in Bucha were Killed by Ukrainian Nazis.” EUvsDisinfo website <<https://euvsdisinfo.eu/report/those-filmed-in-bucha-were-killed-by-ukrainian-nazis>>; “Disinfo: Ukrainian Corpses Move, Stand Up and Avoid Transport in Bucha.” *ibid.* <<https://euvsdisinfo.eu/report/ukrainian-corpses-move-stand-up-and-avoid-transport-in-bucha>> また、ブチャにおける虐殺に関連する約1年間の出来事及びロシア側によるディスインフォメーションをEUvsDisinfoが図にまとめている (“The Bucha Massacre: Mapping a Year of Kremlin Denial,” March 31, 2023. *ibid.* <<https://euvsdisinfo.eu/the-bucha-massacre-mapping-a-year-of-kremlin-denial/>>).

37) 「櫻井よしこ vs 駐日ロシア大使 M・ガルージン」『Hanada』73号, 2022.6, pp.34-35.

38) Володимир Зеленський (@ZelenskyyUa), “Mariupol. Direct strike of Russian troops at the maternity hospital. People, children are under the wreckage. Atrocity! How much longer will the world be an accomplice ignoring terror? Close the sky right now! Stop the killings! You have power but you seem to be losing humanity,” 2022.3.9, 0:23. Twitter <<https://twitter.com/ZelenskyyUa/status/1501579520633102349>>

39) 「荒唐無稽 繰り返すロシア 救助された妊婦さえ「モデルの演技」」『朝日新聞』2022.3.13.

40) “Debunked: Mariupol maternity hospital bombing,” 10 March 2022. Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland website <[https://london.mid.ru/en/press-centre/debunked\\_mariupol\\_maternity\\_hospital\\_bombing/](https://london.mid.ru/en/press-centre/debunked_mariupol_maternity_hospital_bombing/)>

41) “Marianna Vyshemirsky: ‘My picture was used to spread lies about the war’,” *BBC*, 17 May 2022. <<https://www.bbc.com/news/blogs-trending-61412773>>

42) “No, We did not Bomb the Hospital, and it was a Nest of Nazis Anyway,” March 15, 2022. EUvsDisinfo website <<https://euvsdisinfo.eu/no-we-did-not-bomb-the-hospital-and-it-was-a-nest-of-nazis-anyway/>>

る事例として、例えば、一般に入手可能なオープンソースの情報（オシント）に基づいて調査を行う民間の調査組織であるベリングキャットが、ファクトチェックに取り組んで調査結果を公開している<sup>(43)</sup>。また、ニューヨーク・タイムズ紙は、前述のブチャにおける事態について、米国の衛星情報会社マクサー・テクノロジーズが公開したウクライナの占領された地域の複数時点の衛星画像を比較することで、2022年3月にブチャにおいてロシア軍によってウクライナ住民の虐殺が行われたとの分析を報じている<sup>(44)</sup>。

日本に関連する偽情報として、2022年8月16日、岸信夫内閣総理大臣補佐官（当時）を装って複製されたツイッターアカウントから、ウクライナ側を非難するような投稿が行われ、在英ロシア大使館等によって拡散（リツイート）された<sup>(45)</sup>。岸氏は自身の正規アカウントにおいて「フェイク」である旨を投稿し、日本外務省は外交ルートで在英ロシア大使館に抗議してリツイートを削除させたと報じられている<sup>(46)</sup>。また、外務省は、翌17日、ツイッターに「今般、あたかも、ウクライナ軍がザポリヅジャ原子力発電所にミサイル攻撃をした旨を岸信夫総理補佐官がツイッターに書き込んだかのように装う虚偽投稿が在英ロシア大使館のSNSアカウントにリツイートされましたが、このような投稿を岸総理補佐官が発信したとの事実はありません」と投稿した<sup>(47)</sup>。

#### (4) ナラティブの戦い

ナラティブ (narrative) は、「ある事象や課題について読み手や聞き手の認識に働きかけ行動を変えるチカラを持つ」ものであり、多くの場合、「ナラティブは相手を説得し行動変容させ、また時間・因果関係が重要視されている」と説明される<sup>(48)</sup>。また、「効果的なナラティブの要素として、人々が共感を得て、より大きな集団との関連を感じ、自らもそのナラティブに参加できること」が重要であり、「共感を得るための物語は事実でなくてもよいし、根拠なき意見や価値判断でもよい」とされる<sup>(49)</sup>。ロシアについては、ナラティブという概念を、独特の考え方をもちて情報戦に活用しており<sup>(50)</sup>、「実際に生じた事実のうち、彼らの都合のいいことのみを切り取り、彼らの信じる一方的な理念を組み合わせるストーリー（ナラティブ）を作り上げ、正当性を主張するといった情報戦を行っている」との指摘がある<sup>(51)</sup>。

(43) 「雑学！ミリテク広場 ネット集団「ベリングキャット」とは？①—フェイクニュースを暴く新たな情報戦—」『防衛技術ジャーナル』43巻6号, 2023.6, pp.38-47; ウクライナに関する情報がまとめられたベリゲンキャットの公式サイトは以下のとおり。“Ukraine,” Bellingcat website <<https://www.bellingcat.com/tag/ukraine/>>

(44) Browne et al., *op.cit.*(34)

(45) 「「影響工作」の懸念 日本も」『朝日新聞』2023.1.9.

(46) 同上

(47) 外務省 (@MofaJapan\_jp), 2022.8.17, 23:24のツイート <[https://twitter.com/MofaJapan\\_jp/status/1559909123680260097](https://twitter.com/MofaJapan_jp/status/1559909123680260097)>

(48) 政策シンクタンク PHP 総研『日本のナラティブ・パワー—「2025」とその先への戦略—』PHP「日本のナラティブ・パワー」研究会, 2023.2, p.10. <[https://thinktank.php.co.jp/wp-content/uploads/2023/02/pdf\\_narrative\\_20230214.pdf](https://thinktank.php.co.jp/wp-content/uploads/2023/02/pdf_narrative_20230214.pdf)>

(49) 川口貴久「ウクライナ戦争と「ナラティブ優勢」をめぐる戦い」2022.5.21. Synodos ウェブサイト <<https://synodos.jp/opinion/international/28156/>>

(50) 青井千由紀氏は、諸国家は戦略レベルでのナラティブ（戦略ナラティブ）を通じて国際秩序を形成しようとしてきた旨を指摘し、事例として欧米及び日本が「ルールにもとづく国際秩序」を掲げてリベラルな国際秩序を維持しようとしていること、中国が独自の価値観に基づく「中国の夢」に言及し自らを「ブランド」として打ち立てようとしていることを挙げる（青井 前掲注(17), p.110.）。また同氏はロシアのナラティブはオーディエンスを混乱させるための妨害手段として使われることが多く、あからさまな嘘の情報を含む偽情報の類繁かつ多様な利用があると指摘する（同, pp.110, 132-137.）。

(51) 佐々木 前掲注(16), p.24.

ロシアのナラティブの一例として、プーチン大統領が2021年7月12日に発表した論文における主張が挙げられる。プーチン氏は、①ロシア人、ウクライナ人及びベラルーシ人のルーツは古代ルーシの末裔（まつえい）である、②「ロシア人とウクライナ人は1つの民族であり、一体不可分である」、③ソビエト連邦の民族政策によって「ロシア人、ウクライナ人、ベラルーシ人という3つの個別のスラヴ民族の地位が国家レベルで固定化された」のであり「自分をウクライナ人と思っていない人々にもウクライナ化が押し付けられることが往々にしてあった」等と述べている<sup>52</sup>。古代ルーシとは、9世紀末から13世紀に現在のウクライナやロシアなどにまたがる地域を支配したキエフ・ルーシ（キエフ大公国）のことで<sup>53</sup>、研究者らも、民族的にロシア人とウクライナ人は「兄弟」といえる<sup>54</sup>、3つのスラヴ民族が本来は1つの民族であるという考え方はロシアでは伝統的に存在している<sup>55</sup>、と指摘しており、①の見解には、ロシア人にとっての歴史的事実が含まれているといえる<sup>56</sup>。他方で②及び③の見解は、事実とは異なる主張や理念が入れ込まれている<sup>57</sup>。

また、ロシア側は、2022年1月から2月の演説等において、1990年の東西ドイツ統一に関して行われた外交交渉に際して、北大西洋条約機構（North Atlantic Treaty Organization: NATO）は軍事プレゼンスを「東方に1インチも拡大しない」と約束したが、その後中東欧諸国や旧ソ連諸国が次々にNATOに加盟したことで<sup>58</sup>、騙（だま）されたとの趣旨の主張を繰り返している<sup>59</sup>。これについてEUvsDisinfoは、上記の外交交渉の際に、NATOを拡大しないという政治的又は法的拘束力のある約束がなされたことはないと説明している<sup>60</sup>。

上記の2つの例のように、ナラティブには一部事実を含めて理念や主張を展開しているケースがある。東野篤子氏（筑波大学教授）は、「ロシアのプロパガンダでは、「100%の嘘」は稀

52 「プーチン大統領のウクライナ論文〔全文〕（前半）ウラジーミル・プーチン・ロシア大統領の論文〈ロシア人とウクライナ人の歴史的一体性〉」『ロシア政策動向』40巻22号, 2021.11.15, pp.6, 12.

53 「ロシアで起きる「神話化」、史実を無視 プロヒー氏が見た帝国主義」『朝日新聞デジタル』2023.9.7; 「【詳しく】プーチン大統領なぜ執着? キエフ・ルーシの歴史とは」2022.6.17. NHK ウェブサイト <[https://www3.nhk.or.jp/news/special/international\\_news\\_navi/articles/qa/2022/06/17/22839.html](https://www3.nhk.or.jp/news/special/international_news_navi/articles/qa/2022/06/17/22839.html)>; キエフ・ルーシの歴史についてのより詳しい文献として、例えば、松里公孝「ルーシの歴史とウクライナ」塩川伸明編『ロシア・ウクライナ戦争』東京堂出版, 2023, pp.103-126. がある。

54 ロシア情勢研究会「ウクライナ情勢について」『治安フォーラム』27巻11号, 2021.11, p.27.

55 溝口修平「ロシアとウクライナは「一体」都合の良い歴史観が下敷き—プーチン論文—」『エコノミスト』100巻13号, 2022.3.29, p.76.

56 プロヒー（Serhii Plokhy）氏（ハーバード大学ウクライナ研究所長）は、古代ルーシを現在のロシアの前身とみなす「神話」は史実とは異なり、ロシア人と近代のロシア国家は、モンゴルの侵入（1240～1480年）の「タタールのくびき」でキエフ・ルーシが消滅した後に確立しており、同国を起源とする神話化は、19世紀のロシア帝国の時代に起こっていたと述べ、原型とされるキエフ・ルーシが歴史の途上で消滅していること、ロシアがウクライナが独立国家であることを無視していること等を指摘する（「ロシアで起きる「神話化」、史実を無視 プロヒー氏が見た帝国主義」前掲注53）。

57 佐々木 前掲注16, p.24; 溝口 前掲注55, p.76.

58 例えば、1999年にはポーランド、チェコ及びハンガリー、2004年にはバルト三国及び中東欧諸国（スロバキア、スロベニア、ブルガリア、ルーマニア）の計7か国がNATOに加盟している（外務省欧州局政策課「北大西洋条約機構（NATO）について」2023.7, p.3. 外務省ウェブサイト <<https://www.mofa.go.jp/mofaj/files/100156880.pdf>>）

59 “Foreign Minister Sergey Lavrov’s interview on Channel One’s “The Great Game” political talk show, Moscow, January 13, 2022,” Ministry of Foreign Affairs of the Russian Federation website <[https://www.mid.ru/en/foreign\\_policy/news/1794264/](https://www.mid.ru/en/foreign_policy/news/1794264/)>; “Address by the President of the Russian Federation,” February 21, 2022. President of Russia website <<http://en.kremlin.ru/events/president/news/67828>>; “Address by the President of the Russian Federation,” February 24, 2022. *ibid.* <<http://en.kremlin.ru/events/president/news/67843>>

60 “Disinformation About the Current Russia-Ukraine Conflict – Seven Myths Debunked,” January 24, 2022. EUvsDisinfo website <<https://euvsdisinfo.eu/disinformation-about-the-current-russia-ukraine-conflict-seven-myths-debunked/>>; “DISINFO: NATO violated its pledge not to move eastwards.” *ibid.* <<https://euvsdisinfo.eu/report/nato-violated-its-pledge-not-to-move-eastwards>> 日本における主な研究として、以下が挙げられる。吉留公太『ドイツ統一とアメリカ外交』晃洋書房, 2021; 板橋拓己『分断の克服 1989-1990—統一をめぐる西ドイツ外交の挑戦—』中央公論新社, 2022.

であり、事実関係と偽情報、それにロシアの一方的主張が巧妙にミックスされたものが多い」と分析する<sup>(61)</sup>。先述の佐々木孝博氏は、事実と理念を組み合わせた「ナラティブを使った情報戦」では、ファクトチェックによって対応が可能な偽情報とは異なり、事実を争うファクトチェックとは違う次元の対応が必要となると指摘する<sup>(62)</sup>。川口貴久氏（東京海上ディーアール株式会社戦略・政治リスク研究所主席研究員）も、ナラティブに対抗するにはファクトチェックだけでは効果をあげにくいと指摘しており、ウクライナ側がナラティブでロシアに対抗している例として、ゼレンスキー大統領が2022年3月にG7各国の議会において演説をした内容にもナラティブの要素が含まれていると説明する（Ⅱ-2(6) 参照）<sup>(63)</sup>。

## 2 ウクライナによる情報戦

### (1) テクノロジーを活用した市民の参加

ウクライナ政府は、ロシアの軍事侵攻を受けた2022年2月下旬、ロシア・ウクライナで普及しているチャットツールであるテレグラムに「ロシアの侵攻を止める」と題した専用窓口を設け、市民からロシア軍を目撃した場所、時間、具体的に見たもの等を報告してもらい、それを軍が精査して作戦に役立てる仕組みを整えた<sup>(64)</sup>。その後、市民が身の回りの情報を報告するスマートフォンアプリが開発された。

「eVorog」（「敵がいる」という意味）と呼ばれるウクライナ軍への情報提供用のチャットボットは、2022年2月から運用されている<sup>(65)</sup>。30万人以上が使用しており、市民は、ロシア軍の戦車や兵士、さらにスパイ等の不審者を目撃した際に位置情報付きの写真や動画を送信してウクライナ軍に情報を伝えることができる<sup>(66)</sup>。2022年12月時点で、40万件以上の情報が寄せられ、戦闘に生かされているという<sup>(67)</sup>。

「ePPO」と呼ばれるアプリは、低空飛行するためにウクライナ軍のレーダーでは感知できない攻撃に関連する兵器や機体等の位置情報を、市民が軍に通報してミサイルの撃墜につなげる<sup>(68)</sup>。アプリを起動させて、自身が見たものをミサイル、航空機、ドローン、ヘリコプター、爆発の中から選択し、スマートフォンを標的に向けて絵をタッチすると、通報者の位置情報が自動的に添付され、情報が送信される仕組みで、通報のための写真及び動画の撮影や文字の入力の必要はない<sup>(69)</sup>。同アプリの開発者によれば、2022年10月に提供が開始されたePPOは、2023年2月下旬時点で約34万人がダウンロードしており、ミサイルの場合、一度の攻撃で通常1,500～3,000件の情報提供がある<sup>(70)</sup>。

(61) 東野篤子「「プーチン擁護論」の歪みと陥穽」『正論』627号, 2023.11, p.123.

(62) 佐々木 前掲注(16), p.24.

(63) 川口貴久「権威主義国家によるデジタル影響工作と民主主義」一田和樹ほか『ネット世論操作とデジタル影響工作—「見えざる手」を可視化する—』原書房, 2023, pp.210-211.

(64) 「ウクライナ市民 SNSで抵抗戦」『日本経済新聞』2022.3.15.

(65) 「市民のスマホ 軍の「目」に」『毎日新聞』2023.2.24; ミハイロ・フェドロフ「「はじめに」に代えて—ウクライナ副首相兼デジタル変革大臣インタビュー「戦時下でもデジタル政府化は加速する」—」渡部恒雄ほか編『デジタル国家ウクライナはロシアに勝利するか?』日経BP, 2022, pp.5-7.

(66) 「市民のスマホ 軍の「目」に」同上; フェドロフ 同上, pp.6-7; 「ウクライナのDXはいかに防衛戦を支えたか 変革進めた大臣は31歳」『朝日新聞デジタル』2022.7.29.

(67) 「ロシア軍情報40万件 ウクライナ市民の目は力」『朝日新聞』2022.12.26.

(68) 「市民のスマホ 軍の「目」に」前掲注(65); “The “EPPO” APP Has Already Been Downloaded by 330,000 Ukrainian – Developers,” March 30, 2023. Ukraine Media Center website <<https://mediacenter.org.ua/the-eppo-app-has-already-been-downloaded-by-330-000-ukrainian-developers/>>

(69) 「市民のスマホ 軍の「目」に」同上

(70) 同上

これらのアプリは、ウクライナが2020年2月に導入した公共サービスをデジタル化するためのアプリ「Diia」（市民がIDカード、運転免許証等を電子形式で使用できるアプリで、他のアプリとDiiaとを紐付けることで個人認証が可能となる。）を通じた承認がなされた上で使用されており、ロシアなどによって偽情報が寄せられるのを防いでいる<sup>(71)</sup>。

## (2) IT軍及びサイバー義勇兵

ウクライナは、ITに関連して市民や外国人の協力を得た取組を行っている。フェードロフ副首相は、2022年2月26日、ツイッターにIT軍を創設する旨を投稿し、協力者を募った<sup>(72)</sup>。IT軍の参加者は必ずしもサイバーセキュリティ関連の専門家ではなく、IT関連のデザイナー、コピーライター、マーケティング担当者等へもツイッター及びテレグラムを通じて参加が呼びかけられた<sup>(73)</sup>。ウクライナ国民だけでなく外国人も参加しているという<sup>(74)</sup>。ウクライナ政府がIT軍に依頼したい仕事をテレグラムの専用チャンネルに投稿し、参加者はそれを実行する仕組みで、攻撃の指示やDDoSツールなどが共有される<sup>(75)</sup>。サイバー攻撃の手法の中で、IT軍はDDoS攻撃（前述II-1(1)）を推奨している<sup>(76)</sup>。当初の攻撃対象は、ロシアの政府機関、大手銀行、国営メディアのウェブサイトであったが、次第に拡大し、ストリーミングやインターネットバンキングなどのサービスを提供するあらゆるロシアのウェブサイトが標的とされている<sup>(77)</sup>。IT軍は、ロシア国民にウクライナの惨状を伝える情報戦にも注力しており、ロシア国民にメッセージアプリ等で戦争に関する写真や情報を送っている<sup>(78)</sup>。また、ロシアでは検閲の対象となるなどしてテレビでは通常放送されない「ロシア人への声明」と題する動画を定期的に公開している<sup>(79)</sup>。例えば、ウクライナ国内で亡くなったロシア兵の親族にそれを伝えたり、被害を受けたウクライナの建物の映像や亡くなったウクライナ国民の顔がわかる映像をまとめたりした動画がある<sup>(80)</sup>。

サイバー義勇兵は、ウクライナ国防省が、ハッカーやサイバーセキュリティの専門家に対して匿名掲示板で支援を呼びかけて始まったもので、志願者は、コンピュータウイルスの作成やDDoS攻撃などの12分野から自らの得意分野を選んでオンライン上で登録する<sup>(81)</sup>。参加が認められた義勇兵は、電力や水道などの重要インフラをサイバー攻撃から守る防御チーム又はウク

(71) フェードロフ 前掲注(65), pp.6-7; 独立行政法人国際協力機構・三菱UFJリサーチ & コンサルティング株式会社「ウクライナ国行政サービス向上に向けた電子政府の実現に係る情報収集・確認調査ファイナル・レポート」2021.10, pp.65-70. <<https://openjicareport.jica.go.jp/pdf/12366894.pdf>>

(72) Mykhailo Fedorov(@FedorovMykhailo), “We are creating an IT army. We need digital talents. All operational tasks will be given here: <https://t.me/itarmyofuraine>. There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists,” 2022.2.26, 3:38. Twitter <<https://twitter.com/FedorovMykhailo/status/1497642156076511233?lang=ja>>

(73) 松原 前掲注(20), pp.138-139.

(74) 同上, p.142; 「機密データ保管 外国企業と協力 ウクライナデジタル化担当副大臣 イェホール・ドゥビンスキー氏」『読売新聞』2022.8.23.

(75) 松原 前掲注(20), pp.138-139.

(76) 柏村祐「第3部 デジタル国家ウクライナの全貌 第10章 サイバー空間の戦い」渡部ほか編 前掲注(65), p.188.

(77) 松原 前掲注(20), p.139.

(78) 同上, pp.140-141; 柏村祐「ウクライナIT軍「ロシア人への声明」の衝撃～あなたが知らないウクライナIT軍による情報伝達活動～」2022.5. 第一生命経済研究所ウェブサイト <<https://www.dlri.co.jp/files/ld/187785.pdf>>

(79) 柏村 同上, pp.2-3.

(80) 同上, pp.2-3.

(81) 松原 前掲注(20), p.135.

ライナ軍によるロシア軍へのサイバースパイ作戦を支援する攻撃チームに振り分けられ、国防省からの指示に従って活動する<sup>82</sup>。2022年3月下旬の情報によれば、1,000人近くのサイバー義勇兵のうち約4割が外国人だという<sup>83</sup>。

### (3) 通信手段の確保—スターリンク—

ロシアからの攻撃を受けながら、ウクライナが前述のような対応を取ることができた1つの理由は、通信インフラを維持することができたからである。ウクライナは、2014年にロシアがクリミアに軍事攻撃をした際にサイバー攻撃対策ができていなかったことを教訓に、2021年までに通信インフラの分散化を進め、4,900以上のインターネット・サービス事業者を国内に抱えており、サイバー攻撃や物理的な攻撃を受けた場合にも、一度にすべての通信がダウンさせられる可能性は低く抑えられていた<sup>84</sup>。

2022年2月24日、ロシアが軍事侵攻を開始する約1時間前、ウクライナ軍が使用する衛星通信網KA-SATは、ロシアによるサイバー攻撃を受けた<sup>85</sup>。標的とされたのは、KA-SAT衛星そのものではなく、衛星の管理を担うヴィアサット社の関連企業が運用する消費者向けネットワークの一部で、モデムのセキュリティの脆弱（ぜいじゃく）性を突いて管理用ネットワークに侵入された<sup>86</sup>。2月26日には、フェードロフ副首相がツイッターを用いてマスク（Elon Musk）氏（スペースX社CEO）に通信衛星スターリンクの提供を要請し、半日足らずのうちにウクライナにおいてスターリンクのサービスが利用可能となった<sup>87</sup>。スターリンクは、小型衛星で通信電波を中継するため、衛星及び通信用の小型アンテナ（直径約55センチ）があれば、サービス提供地域のどこでもインターネットが使用できる<sup>88</sup>。すぐに提供に至ったのは、ウクライナのデジタル転換省とスペースX社との間で、戦争開始の数か月前からスターリンクの提供に関する交渉が行われていたからだとされる<sup>89</sup>。2022年4月の報道によれば、ウクライナのネット通信のデータ量は、侵略前の約8割の水準を維持していた<sup>90</sup>。

### (4) ハント・フォワード作戦

米国のサイバー軍司令官を務めるナカソネ（Paul Nakasone）氏によれば、ハント・フォワー

82) 同上, p.136.

83) 同上, p.136.

84) 同上, pp.29-30.

85) European Space Policy Institute, “The War in Ukraine from a Space Cybersecurity Perspective,” October 2022. <<https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Report-84.pdf>>

86) *ibid.*; “KA-SAT Network cyber attack overview,” March 30, 2022. Viasat website <[https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview#:~:text=At%20approximately%200302%20UTC%20on,SAT%20consumer-oriented%20network%20partitions.](https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview#:~:text=At%20approximately%200302%20UTC%20on,SAT%20consumer-oriented%20network%20partitions.;)>; 青葉やまと「ロシアのサイバー攻撃、ヨーロッパ全域の衛星モデムやドイツの風力発電2000基を監視不能に」2022.4.11. Newsweek 日本版ウェブサイト <[https://www.newsweekjapan.jp/stories/world/2022/04/post-98482\\_1.php](https://www.newsweekjapan.jp/stories/world/2022/04/post-98482_1.php)>

87) Mykhailo Fedorov(@FedorovMykhailo), “@elonmusk, while you try to colonize Mars — Russia try to occupy Ukraine! While your rockets successfully land from space — Russian rockets attack Ukrainian civil people! We ask you to provide Ukraine with Starlink stations and to address sane Russians to stand,” 2022.2.26, 21:06. Twitter <<https://twitter.com/FedorovMykhailo/status/1497543633293266944>>; Elon Musk(@elonmusk), “Starlink service is now active in Ukraine. More terminals en route,” 2022.2.27, 7:33. *ibid.* <<https://twitter.com/elonmusk/status/1497701484003213317>>

88) 「衛星ネットサービス「スターリンク」露軍に対抗 実戦投入」『毎日新聞』2022.5.20. なお、アンテナは、スペースX社の寄付や米国国際開発庁の支援を受けてウクライナに大量に送られた（同）。

89) 松原 前掲注(20), p.117.

90) 「対口戦 通信が命綱 ウクライナの対外発信支える 軍事支援と両輪に」『日本経済新聞』2022.4.26.

ド作戦 (Hunt Forward Operation) とは、要請を受けた国へ8~10人のチームを派遣し、派遣先の国と共同でネットワークの追跡を行い、その情報を産業界とも共有するもので、2018年に開始されてから2023年3月までに、22か国の70のネットワークにおいて47のミッションが実施されている<sup>91)</sup>。

米国は、2021年12月から2022年2月までの約90日間にわたり、ウクライナ政府の同意を得て、同国に米海軍と米海兵隊の合同チームをハント・フォワード作戦として派遣した<sup>92)</sup>。これにより、両国のサイバー専門家が共に悪意あるサイバー攻撃の搜索作業を行うことで、ウクライナはネットワーク上の潜在的脅威を特定して対処し、重大度が高い順に脅威を軽減することができた<sup>93)</sup>。2022年1月中旬にロシアが破壊的なサイバー攻撃を開始したとき、ウクライナに滞在していた米国チームは、ウクライナ側と緊密に連携し、攻撃の分析を支援するとともに、その情報を米国内の関係省庁や国土防衛に係る業界パートナーと共有した<sup>94)</sup>。米国チームがウクライナから撤退した後も協力は続けられており、サイバー攻撃の痕跡を示す情報 (Indicator of Compromise: IoC) やマルウェアの情報といったサイバーに関する知見の情報共有が行われている<sup>95)</sup>。

#### (5) ウクライナによるIT企業への協力要請—重要データのクラウド移行—

ロシアによる軍事侵攻の可能性が高まっていたのを受けて、ウクライナ政府は、首都キーウにある政府のサーバーからデータを消去してキーウの外にデータを移動させたという<sup>96)</sup>。ウクライナには長年にわたり、政府によるパブリッククラウド上におけるデータ処理及び保管を禁止するデータ保護法があったが<sup>97)</sup>、2022年2月17日、ウクライナ議会は、政府のデータを既存のサーバーからパブリッククラウドに移動できるよう法改正を行った<sup>98)</sup>。同月24日、ロンドンのウクライナ大使館においてウクライナの駐英大使とアマゾン・ウェブ・サービス (AWS) スタッフとの打合せが行われ、戸籍、土地の登録情報、納税記録、銀行情報、教育関連情報、汚職防止データベース、ウクライナ最大の金融機関プライベート銀行などの数十の企業データを移行することが決定された<sup>99)</sup>。数日中に、AWSの「スノーボール」——大量のデータを格納してクラウドに移すことができるスーツケースのような形の装置——がポーランド国内においてウクライナ側に引き渡されてキーウに届けられ、ウクライナ側は対話アプリを通じてAWSの支援を得ながら暗号化したデータを「スノーボール」に保存してバックアップを取り、データ

91) “House Armed Services Subcommittee on Cyber, Innovative Technologies and Information Systems Holds Hearing on Defense Cyberspace Operations,” March 30, 2023. テキストは Lexis の CQ Transcriptions で入手した。

92) 渡部ほか 前掲注(14), pp.145-146; “Before the Invasion: Hunt Forward Operations in Ukraine,” Nov. 28, 2022. National Security Archive website <<https://nsarchive.gwu.edu/sites/default/files/documents/rmsj3h-751x3/2022-11-28-CNMF-Before-the-Invasion-Hunt-Forward-Operations-in-Ukraine.pdf>>

93) “Before the Invasion: Hunt Forward Operations in Ukraine,” *ibid.*

94) *ibid.*

95) *ibid.*

96) 松原 前掲注(20), p.44.

97) パブリッククラウドとは、独自の環境を整備するのではなく、クラウドサービス提供事業者が構築した環境を他の利用者と共同利用するクラウドサービスのことである (「パブリッククラウドとは? 機能や活用シーン・企業の導入事例など」2022.8.10. NTT 東日本ウェブサイト <<https://business.ntt-east.co.jp/content/cloudsolution/column-314.html>>)。

98) Microsoft, “Defending Ukraine: Early Lessons from the Cyber War,” June 22, 2022, p.5. <<https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK>>

99) 松原 前掲注(20), pp.45-46; 「常識覆すアマゾンの雪玉作戦 ウクライナ個人情報はこうして救われた」『朝日新聞デジタル』2023.4.21.

は安全な場所に移されてからクラウドに保存された<sup>(100)</sup>。データ移行の際には、マイクロソフトやグーグルも無償でクラウドサービスを提供した<sup>(101)</sup>。なお、松原実穂子氏（NTT チーフ・サイバーセキュリティ・ストラテジスト）は、これだけ大規模なデータ移行を2、3日の調整で実現するのは困難であり、軍事侵攻の数か月前から少なくともIT・サイバーセキュリティ業界においては、大掛かりなデータ移行のために国際的な官民の調整が進められていたのではないかと推察している<sup>(102)</sup>。

## (6) ゼレンスキー大統領の発信

ゼレンスキー大統領は、SNSを活用した情報発信により、ウクライナ国内を偽情報の混乱から守り士気を高める一方で、各国議会においてオンライン演説を行うなど、ウクライナへの支持を集める象徴となってきた。ロシアによる侵略開始当初、ロシアのメディアは、ゼレンスキー大統領がキーウからリビウへ逃げたと報じたが<sup>(103)</sup>、ゼレンスキー大統領は、キーウの中心地で政権幹部たちと自撮りした動画を自らツイッターなどのSNSに投稿し、ウクライナの独立と国を守る旨を訴えて偽情報を打ち消した<sup>(104)</sup>。この動画に登場したポドリャク（Mykhailo Podolyak）大統領府長官顧問は、後に動画はゼレンスキー氏の提案により撮影された旨を述べている<sup>(105)</sup>。

2022年3月、ゼレンスキー大統領は各国の議会においてオンライン形式の演説を行い、ウクライナ支援への支持を高めた<sup>(106)</sup>。日本の国会においては、東日本大震災による原発事故を想起させるかのように、1986年の事故後に閉鎖されたチョルノービリ原子力発電所がロシア軍に制圧されたことやザポリッジャ原子力発電所が攻撃を受けたことを挙げ、「人々は、住んでいた故郷、子ども時代を過ごした故郷、住み慣れた故郷に戻する必要があります。皆さんにもきつとこの気持ちがかかります」と訴えた<sup>(107)</sup>。英国、米国及びその他の国々でも、国ごとの歴史に則した例えを挙げ、当地における有名な演説を引用するなど、「聞き手と感情の連帯を作ることに力点を置いている」と評される<sup>(108)</sup>。より多くの支援を求めるゼレンスキー大統領の演説は、西側諸国の国内世論に訴え、国内から各国政府に対してウクライナを支援するよう圧力をかけようとしたものであるとの分析もある<sup>(109)</sup>。

(100) 松原 同上, pp.45-46; 「ウクライナから重要データ「避難」 アマゾン支援の舞台裏」『日本経済新聞』2022.12.4.

(101) 松原 同上, p.46; Microsoft, *op.cit.*(98), p.5.

(102) 松原 同上, p.47.

(103) “Zelensky Has Fled Kiev for Lvov, Russian State Duma Speaker Says,” *Sputnik International*, 26.02.2022. <<https://sputnikglobe.com/20220226/zelensky-has-fled-kiev-for-lvov-russian-state-duma-speaker-says-1093390487.html>>

(104) 「「私たちはここにいる、独立を守る」 首都からウクライナ大統領が政府幹部と」*BBC News*, 2022.2.26. YouTube <<https://www.youtube.com/watch?v=FvymJO4idHs>>

(105) 「追跡 大統領演説、ライターは誰？ ウクライナ、共感呼ぶメッセージ」『毎日新聞』2023.8.11.

(106) 田中理「第5部 地政学から予想される欧州の変貌 はじめに ゼレンスキーとは何者か？」渡部ほか編 前掲注(65), pp.316-318.

(107) 「ゼレンスキー・ウクライナ大統領演説（仮訳）」2022.3.23. 参議院ウェブサイト <<https://www.sangiin.go.jp/japanese/ugoki/r4/220323-2.html>>; 「制裁強化と復興支援 呼びかけ ゼレンスキー大統領 国会議員らに」『朝日新聞』2022.3.24.

(108) 「一体感醸す言葉重ね ゼレンスキー氏 国会演説」『毎日新聞』2022.3.24; 福田充「ゼレンスキーの情報戦は世界の流れを変えるか」『潮』759号, 2022.5, pp.74-76.

(109) Paul Adams, “‘Shame on you’: How President Zelensky uses speeches to get what he needs,” *BBC*, 24 March 2022. <<https://www.bbc.com/news/world-europe-60855280>>



### 3 ロシア及びウクライナ以外の主体の動向

#### (1) 米英の「開示による抑止」

米国及び英国の両政府は、2021年12月から2022年2月24日まで、ロシアによるウクライナへの軍事侵攻の兆候を示す機密情報を公表した<sup>(110)</sup>。本稿のII-1(2)に挙げたように、米国がロシアの偽旗作戦を公表したことも、機密情報の開示の一部といえる。

米国による機密情報の公表に関しては、タイガーチーム——2021年11月にホワイトハウスの国家安全保障会議に設けられた組織で、国防省、国務省、エネルギー省、財務省、国土安全保障省、国際開発庁、情報機関のスタッフが関与する——が大きな役割を果たした<sup>(111)</sup>。タイガーチームが戦略の検討を担い、ロシアによるウクライナ侵略の開始前に様々なパターンのシナリオを作成して米国の対応を検討したことで、ロシアが拡散しようとする情報が伝播（でんぱ）力を得る前にロシア側の意図を周知させることが可能となり、ロシアの情報戦の勢いを削ぐのに役立ったと、2022年2月14日に報じられている<sup>(112)</sup>。また、同月17日の報道によれば、ロシアが侵略を開始する前に米国から欧州へも報告が行われ、起こり得る事態への対応策及びロシアとの情報戦に対抗するために米国が得たロシアの動向の情報を開示していく方針が固められていた<sup>(113)</sup>。

瀬戸崇志氏（防衛研究所政策研究部グローバル安全保障研究室研究員）は、米国によるロシア軍のウクライナ国境付近における動向を示した衛星写真等の分析資料の公表、英国によるロシアのウクライナの政権転覆工作・傀儡（かいらい）政権樹立計画の存在の公表といった主な機密情報の公開をまとめている<sup>(114)</sup>。情報を公開することで相手側の行動を抑止しようとする戦略は、「開示による抑止」（Deterrence by disclosure）と呼ばれる<sup>(115)</sup>。

#### (2) EUvsDisinfo

先述（II-1(3)及び(4)）のEUvsDisinfoは、ロシアによる欧州連合（European Union: EU）、EU加盟国及び近隣国に影響を及ぼすディスインフォメーション・キャンペーン（偽情報の拡散・流布）に対応するため2015年に開始された、EU外務・安全保障政策上級代表の権限の下に置かれている欧州対外行動庁（European External Action Service）のプロジェクトであり、15か国語のデータ分析及びメディア監視サービスを活用して、EU加盟国及び東方パートナーシップを結ぶ国々（アルメニア、アゼルバイジャン、ベラルーシ、ジョージア、モルドバ及びウク

(110) 瀬戸崇志「ロシアのウクライナ侵攻と米英両国のインテリジェンス公表政策—情報機関の「ジレンマ」と2014年以降の安全保障協力の「系譜」—」『NIDS コメンタリー』224号, 2022.5.26, p.1. <<http://www.nids.mod.go.jp/publication/commentary/pdf/commentary224.pdf>> 関連する論考として例えば、小島吉之「ロシアのウクライナ侵攻（2022年2月）と米国の情報開示—情報による戦争抑止の可能性に関する考察—」『Roles Report』22号, 2023.3. <<https://roles.rcast.u-tokyo.ac.jp/uploads/publication/file/49/publication.pdf>>; 小谷賢「ウクライナ戦争における欧米の対ウクライナ支援—機密情報と武器供与の観点から—」『国際武器移転史』15号, 2023.1, pp.29-41; 高木耕一郎「米国が制したウクライナ情報戦—戦争の「ドライブ・レコーダー」としての公開情報—」『外交』80号, 2023.7・8, pp.34-39がある。

(111) Ellen Nakashima and Ashley Parker, “Inside the White House Preparations for a Russian Invasion,” *Washington Post*, February 14, 2022; 「米、対ロ機密を積極開示 大統領直轄チーム 侵攻抑止狙う」『日本経済新聞』2022.2.17.

(112) Nakamura and Parker, *ibid.*; 「米、対ロ機密を積極開示 大統領直轄チーム 侵攻抑止狙う」同上

(113) Nakamura and Parker, *ibid.*; 「米、対ロ機密を積極開示 大統領直轄チーム 侵攻抑止狙う」同上

(114) 瀬戸 前掲注<sup>(110)</sup>, p.3.

(115) 「ウクライナ軍事侵攻 熾烈な情報戦 攻撃開始9時間前に何が」2022.2.25. NHK ウェブサイト <<https://www3.nhk.or.jp/news/html/20220225/k10013500661000.html>>; 渡部悦和「ロシア・ウクライナ戦争の教訓」『安全保障を考える』810号, 2022.11.1, pp.14-15. <[http://www.anpokon.or.jp/pdf/kaishi\\_810.pdf](http://www.anpokon.or.jp/pdf/kaishi_810.pdf)>

ライナ)<sup>(116)</sup>に広がる親ロシア政府のメディアから発信された偽情報を特定し、まとめて公表している<sup>(117)</sup>。ロシアによるウクライナ侵略において、紛争の当事者以外が情報の真偽を判断する活動が行われたことは、欧州を意図的に狙って発信された多くの偽情報を発見し、欧州におけるロシアの偽情報の影響に関する意識を大きく高めたとされる<sup>(118)</sup>。

## おわりに

ロシアによるウクライナ侵略は、陸海空の領域にとどまらず、DDoS 攻撃や通信妨害、電力等の重要インフラシステムへのサイバー攻撃、偽情報の流布やナラティブの戦い等、多岐にわたる領域に及んでいる。ロシア、ウクライナ等が展開してきた情報戦は、SNS 等によって世界中でリアルタイムの情報共有が可能となり、エネルギー、IT、銀行等の社会インフラ及び国家が管理する個人情報情報が情報システムに依存している現代社会において、情報戦が行われることによりどのような事態が生じ得るのか、そしてどのような対応が考えられ得るのか、参考となる多くの事例を提示している。

(あおい よしえ)

---

(116) EU は、2004 年から、安定、安全保障、福祉を強化することで EU 拡大の利益を近隣諸国と共有することを目的とする欧州近隣諸国政策 (European Neighbourhood Policy: ENP) を行っていたが、異なる価値観や文化、歴史を有する地中海諸国と旧ソ連諸国を ENP という同じ枠組みの中で扱うことへの批判があり、2008 年から、地域ごとの事情を考慮した上で各国の状況に適応した個別の政策と全体的な政策を同時並行させる方針への転換が行われ、ENP 対象国のうち括弧内に挙げた旧ソ連 6 か国を対象とする「東方パートナーシップ」という枠組みが設けられている (佐藤良輔「近隣諸国政策」坂井一成・八十田博人編『よくわかる EU 政治』ミネルヴァ書房、2020, pp.112-113.)。

(117) “About.” EUvsDisinfo website <<https://euvsdisinfo.eu/about/>>

(118) 南亮一「EU 域内の国民投票運動におけるオンライン広告規制の動向—政治広告の透明性の確保及び偽情報対策の観点から—」国立国会図書館調査及び立法考査局『諸外国の国民投票運動におけるオンライン広告規制』(調査資料 2022-1-a 基本情報シリーズ 29) 国立国会図書館, 2023, p.133. <<https://doi.org/10.11501/12767880>>