研究レポート

新国家安保戦略とサイバー、情報戦への対応

2024-02-14
大澤淳（中曽根平和研究所主任研究員）

「新領域リスク」研究会 FY2023-2号
「研究レポート」は、日本国際問題研究所に設置された研究会参加者により執筆され、研究会での発表内容や時事問題等について、タイムリーに発信するものです。「研究レポート」は、執筆者の見解を表明したものです。

2022年12月に決定された国家安全保障戦略では、サイバー攻撃の脅威が急速に高まっているという認識の下、我が国を全方位でシームレスに守るための取り組みの強化として、サイバー安全保障分野での対応能力を欧米諸国と同等以上に向上させるとの記述が盛り込まれた。また、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃の恐れがある場合、これを未然に排除し、被害の拡大を防止するために能動的サイバー防御を導入することが謳われている。能動的サイバー防御に関しては、法整備、運用の強化、体制の整備が行われることが示され、23年1月にサイバー安全保障法制準備室が内閣官房に設置された。

国家安全保障戦略におけるサイバー安全保障への危機感の背景には、2022年2月に始まったロシア・ウクライナ戦争において、ハイブリッド戦争と言われる現代戦が行われていることが挙げられる。ハイブリッド戦争では、戦車やミサイルを使った通常戦の前に、機能破壊型のサイバー攻撃や情報操作型のサイバー攻撃である情報戦が行われる。そのため、平時に情報空間で危機が進行することが特徴である。ロシア・ウクライナ戦争では、第一段階の情報戦が2014年以降、親欧のウクライナの政治体制の信頼を貶めるために行われ、第二段階のサイバー攻撃が、通常戦の直前の2022年1月中旬から三波にわたって行われた。

第一段階の情報戦では、ウクライナのゼレンスキー政権がネオ・ナチの政権であるというイメージを植えつけるため、ゼレンスキー大統領がナチスドイツの鉤十字(ハーケンクロイツ)のマークが描かれたウクライナのサッカー・ナショナルチームのユニフォームをもらって喜ぶ偽画像や、ウクライナ軍の部隊やアゾフ連隊が好んで鉤十字のマークを多用している偽写真がSNS上で

流布された。欧米諸国に対しては、ロシアのウクライナ侵攻の原因が冷戦後のNATOの東方拡大にある、との偽情報を含む物語(ナラティブ)が集中的に流されている。

「虚偽のニュースは真実よりも有意に遠く、速く、深く、広く拡散し、その効果は、テロ、自然災害、科学、都市伝説、金融に関する虚偽のニュースよりも、政治に関する虚偽のニュースにおいて顕著である」ことが米国MITの研究グループによって明らかにされている。ロシア・ウクライナ戦争でも開戦直後の2月25日に、「ゼレンスキー大統領がキエフから逃亡した」との偽情報がロシアによって流された。このニュースは瞬く間にネット空間で広まったが、数時間後の25日深夜に、ゼレンスキー大統領は自分のスマートフォンで映像を自撮し、「私たちはキエフにいて独立を守る」とYouTubeやFacebookなどの自身のアカウントで宣言した。このゼレンスキー大統領の素早い動画配信がなければ、ウクライナ国民の国土防衛の士気は早期に崩壊し、ロシア軍はキエフをなんなく占領することができたであろう。

ロシアのゲラシモフ参謀総長は、2013年2月の現代戦に関するスピーチの中で、「現代戦においては戦争のルールが変わり、政治的・戦略的目標を達成するための非軍事的手段の役割は大きくなり、多くの場合、その効果は武器の力を上回っている。情報空間は、敵の戦闘力を低下させる非対称的な可能性を大きく広げる」と指摘している。そのためロシアは平時からの情報戦・影響力工作に力を入れており、エストニア対外情報庁の2021年の年次報告によれば、さまざまな情報戦の手法を行使していると分析されている。その手法としては、①メディアサイトの乗っ取りとフェイクニュースの流布、②ハッキングとリーク、③DDoS攻撃によるサービス妨害、④ウェブサイトの改竄などが行われるとされ、我々が通常情報戦で思い浮かべるような偽情報の流布だけでなく、情報窃取やDDoSなどのサイバー攻撃も組み合わせた手法が用いられている。

ロシアのこういった情報戦は、認知領域の戦いであり、その目的は相手国が内包する矛盾を見極め、その矛盾を偽情報などの手段を用いて増幅し、社会の亀裂を拡大することにより相手を弱体化させるという点にある。情報戦の結果として相手社会が弱体化すれば、国際社会におけるロシアの立ち位置が相対的に向上するとの考えを有していると言われている。例えば西欧社会に対しては、イスラム移民の流入による社会不安の増大を格好の機会と捉え、この亀裂を情報戦で利用することによって、反イスラム移民のナショナリズムを喚起し、極右の台頭を促すことによって、西欧の多元的民主主義の安定性を崩そうとしている。

民主主義諸国における選挙は、このようなロシアの情報戦の格好のターゲットであり、2016年の米国大統領選挙では、SNS上での偽情報の流布、ハッキングによる機密情報のリーク、選挙システムへのサイバー攻撃などが行われた。その結果、黒人の投票率が12年の大統領選挙を6%下回るなど顕著に低下し、民主党支持層の投票行動に一定の影響を与えた。また、この選挙戦を通じて、郵便投票制度や開票集計システムなどに対する偽情報も流布されたため、米国の選挙制度や民主主義制度自体に対する信頼が揺らぎ、陰謀論を信奉する「Qアノン」が台頭するなど、米国社会の信頼や統合を毀損することとなった。それ以外にも、2016年のBrexitに関する英国での国民投票、2017年のフランスの大統領選挙、同年のドイツの総選挙でも、ロシアによる情報戦が観測されている。

ロシアと同様に中国も認知領域を戦場と認識しており、近年では認知空間での優位性を確保する「制脳権」という言葉が、軍関係の文献でも頻繁に登場するようになっている。台湾の2021年の国防報告書によれば、こういった中国の認知戦の手段は多岐にわたり、①公式メディアを使った対外宣伝方式、②SNSへの大量の書き込みによる民族主義者方式、③コンテンツファームを利用した情報の流布、④現地の協力者を用いた情報操作などが行われている、と分析されている。実際に過去台湾における総統選挙や統一地方選挙では、中国によるこのような情報戦が観測されており、今年1月の総統選挙でも、中国による偽情報の流布が行われている。

サイバー攻撃の点でもわが国に対するロシア・中国・北朝鮮による攻撃の増加が観測されており、とくに2023年はG7サミット前に、ロシアから政府機関、地方自治体、交通機関などを標的としたDDoS攻撃の増加が観測された。

このような平時から危機が進行する情報戦やサイバー攻撃に対応するためには、能動的サイバー防御が不可欠となっている。能動的サイバー防御は、まず①情報収集として、通信傍受、メタ・データの収集などを用いた、サイバー攻撃に関するデータの収集と観測、②分析・特定として、技術手法を用いた攻撃者の分析・特定、③対応決定として、分析から得られた状況判断を基にして攻撃者への技術的・政策的対応の決定、④対応実施として、攻撃軽減のための技術的措置や政策対応の実施、といった一連のオペレーションのサイクルを24時間365日実施する必要がある。このような能動的サイバー防御を行うためには、国家安全保障戦略で掲げられた行うための法整備、体制整備が急務となっている。

2024年1月30日脱稿