2024 年 7 月 16 日

情報空間のリスク研究会
「中国による情報戦」「中国のサイバー攻撃およびサイバー空間における情報戦・認知戦と生成 AI 技術の活用」
実施報告

中曽根平和研究所・情報空間のリスク研究会では 2024 年 7 月 16 日、研究会座長の大澤淳（当研究所主任研究員）と京都先端科学大学准教授の土屋貴裕委員のご報告をもとに、議論を行いました。要旨は以下の通りです。

大澤淳座長は、「中国による情報戦」と題して報告を行った。

まず、ハイブリット戦の様相として、日本においては情報戦・心理戦とサイバー戦の担当部署が分かれているが、中国やロシアからの攻撃が両者の組み合わせによって行われている現状を概観した。そのうえで、情報戦のみならずサイバー戦も合わせて見ていく必要があり、また最近のサイバー攻撃の情勢を踏まえ、サイバー情報把握(CSA)の重要性が高まっていることを指摘した。

つぎに、中国の認知領域における戦いの概要を説明した。「制脳権」というコンセプトが現れて以降、例えば中国共産党と関係するアクターは、X(旧 Twitter)上で米国民を偽装したボットアカウントを用いて、アメリカの政治問題、社会問題などの国内問題の偽情報を流布することで米国の不安定化を促してきた。しかし、こういった状況に対して欧米諸国が対処を始めたのはここ 2～３年のことであり、対処が遅れていると言える。2023 年 9 月に発表された米国務省の中国情報戦レポートでは、中国が情報空間におけるナラティブを支配しようとしていることや、情報操作がプロパガンダ、偽情報、検閲などを含み多岐に渡っているという分析がなされている。また、ウクライナ戦争においても、中国はロシアの偽情報を情報空間において増幅させる活動を行なってきた。こういった情報工作の実施主体としては中国中央宣伝部や中央統戦部が挙げられ、特に日本を含む諸外国にて平時に見られる偽情報の拡散に寄与しているのが中央宣伝部であり、昨年問題となった福島の処理水問題についても中央宣伝部によるキャンペーンではないかとの疑いがある。

また、単に偽情報の流布だけでなく、サイバー攻撃と組み合わせたキャンペーンが展開されていることについても説明があった。ロシア型の複合型情報戦（サイバー攻撃と偽情報の流布）では、トロール部隊を使った偽情報拡散に加え、DDoS 攻撃によるサービス妨害やハッキング・リークといったサイバー攻撃手法も併用されている。中国による複合型情報戦の具体例として、2022 年のペロシ米下院議長訪台に伴う DDoS 攻撃の増加やハッキングによるメッセージ改竄などのが挙げられた。

台湾総統選では、「米軍は台湾に来援しない」「米国は台湾国内に生物兵器研究所を設置する」といった同盟国の信頼失墜や同盟関係の分断を試みるナラティブを含んだ偽情報の流布が行われた。こういった類の偽情報は台湾のみならず韓国や日本においても確認されている。例えば、韓国では中国企業が運営するニュースおまとめサイトが新型コロナウイルスに関連して「ワシントンは同盟国を実験場として利用している」といった偽情報を含む記事を掲載した。また、カナダのトロント大

学による調査では、同様のニュースおまとめサイトが日本においても運営されていることが指摘された。このような情報戦に対処するためには、攻撃者のナラティブを認識した上で SNS 空間を分析することや、ナラティブの元となる時事的話題に注意した上で、拡散ツール・経路に注視することが重要となる。

また、人工知能（AI）を利用した影響力工作についても指摘があった。2024 年 4 月に発表されたマイクロソフト社のレポートによると、中国の攻撃主体は、AI 生成コンテンツ・AI 強化コンテンツを影響力工作に利用しており、影響力工作主体は米日韓台において、AI 生成コンテンツ（映像、音声、ミームなど）を増幅し、中国の戦略的ナラティブの浸透に利用されている。具体的には、Storm-1376 として知られる中国共産党関連のアクターが、2023 年冬ごろ、台湾の総統選と立法委員会選挙を標的として、AI を利用した影響力工作を展開した。これは国家行為主体が外国の選挙に影響を与えようとして AI コンテンツを使用した初めてのケースと言える。

つぎに、土屋貴裕委員は「中国のサイバー攻撃およびサイバー空間における情報戦・認知戦と生成 AI 技術の活用」と題して報告を行った。

冒頭、頻発するサイバー攻撃の現状について説明があった。ほぼ全ての企業がサイバー攻撃の標的となっているなど国家が関与するサイバー攻撃が顕在化する中、攻撃手法が洗練されており、また、攻撃者優位でセキュリティが後手に回っている状況について言及がなされた。

まず中国によるサイバー攻撃及び情報戦・認知戦のための活動組織として、サイバー攻撃については国家安全部と人民解放軍網絡（サイバー）空間部隊、情報戦・認知戦については国家公安部、国家安全部、人民解放軍信息（情報）支援部隊などが主なアクターであると考えられているが、人民解放軍戦略支援部隊の組織改編により現在は明らかになっていない部分も多い。これら組織が関与して中国のナラティブ形成に強く取り組んだと見られる事例として、「台湾総統戦への介入」、「一帯一路構想と連動したサイバー空間の利用」、そして「サイバー空間におけるプロパガンダ活動」が指摘された。

生成 AI 技術を活用した情報戦・認知戦も確認されている。例えば、2022 年のペロシ米下院議長が台湾を訪問した後に行われた中国による軍事演習前後から、ディープフェイクをはじめとする生成 AI などの新たな技術と、新しいオンライン・コミュニティ・プラットフォームの多様なチャネルを利用した新たな手法が使用され始めた。ディープフェイク動画については、中国国内のみならず欧米諸国に対する拡散も見られたものの、現在の精度であれば本物とフェイクを見分けることが可能で、実際、台湾総統選で確認された事例でもすぐにデバンキングが行われた。しかし、技術の進歩によって、近い将来に AI を用いるなどしなければこれらのコンテンツを見分けられない時代が訪れる可能性が指摘された。

また、AI を使ったアバターの実用化も行われている。中国のプラットフォームではすでに AI アナウンサーが 20～30 社で登場しており、2023 年のオーストラリア戦略政策研究所（Australian Strategic Policy Institute）の報告書によると、外国人アバターを用いることでより広く偽情報を浸透させる試みが確認されている。これらの AI 生成人物を使った宣伝、偽情報拡散は日米や台湾のみならず、YouTube のアカウント等を用いてヨーロッパに対しても行われている。また、TikTok 上ではロシアの軍人を模したアバターのディープフェイクによって中国国内世論に影響を与える

ような動画も拡散された。

そのほかの事例として、さまざまなアカウントを用いてプラットフォーム横断的に展開される「スパムフラージュ」(Spamouflage) は 2019 年の香港の民主派運動後も継続した活動が確認されている。また、CNN の報道によれば、ウクライナ人女性の顔を用いたディープフェイク動画が中国国内の世論に影響を与えるために利用されていた。これに対して、この報道に登場する AI 生成の中国人アバターが、実在する人物であると訴える反論動画が中国側から発信される事案も紹介された。

以上の報告を受けて、質疑応答では、「戦略的コニュニケーションとサイバーセキュリティの共通項」や「中露の連携や相互の学習状況」「今後中国が日本に対して行う可能性のあるナラティブ」について、また「中国国内における情報工作の役割分担やメカニズム、コントロールの主体」「オンライン空間に加えて現地のナラティブ等ローカルレベルの事象との関係」、そして「ソーシャルメディア上の情報をマスメディアが報道することで更に情報が拡散されることを踏まえて、マスメディアの役割や報道の仕方」について、コメントが交わされた。