第3節 サイバー領域をめぐる動向

1 サイバー空間と安全保障

インターネットは、様々なサービスやコミュニティが形成され、新たな社会領域（サイバー空間）として重要性を増している。このため、サイバー空間上の情報資産やネットワークを侵害するサイバー攻撃は、社会に深刻な影響を及ぼすことができるため、安全保障にとって現実の脅威となっている。

サイバー攻撃の種類は、不正アクセス、マルウェア（不正プログラム）による情報流出や機能妨害、情報の改ざん・窃取、大量のデータの同時送信による機能妨害のほか、電力システムや医療システムなど重要インフラのシステムダウンや乗っ取りなどがあげられる。また、AIを利用したサイバー攻撃の可能性も指摘されるなど、攻撃手法は高度化、巧妙化している。

軍隊にとっても、サイバー空間は、指揮中枢から末端部隊に至る指揮統制のための基盤であり、サイバー空間への依存度が増大している。サイバー攻撃は、攻撃主体の特定や被害の把握が容易ではないことから、敵の軍事活動を低コストで妨害できる非対称な攻撃手段として認識されており、多くの国がサイバー攻撃能力を開発しているとみられる。

2 サイバー空間における脅威の動向

諸外国の政府機関や軍隊のみならず民間企業や学術機関などに対するサイバー攻撃が多発しており、重要技術、機密情報、個人情報などが標的となっている。また、高度サイバー攻撃（APT）は、特定の組織を執拗に攻撃するとされ、長期的な活動を行うための潤沢なリソース、体制や能力が必要となることから、組織的活動であるとされる。

Advanced Persistent Threat

このようなサイバー攻撃に対処するために、脅威認識の共有などを通じて諸外国との技術面・運用面の協力が求められている。こうしたなか、米国は、攻撃主体が悪意のあるサイバー活動によって非対称な優位性を獲得し、重要インフラを標的にすることで、米国の軍事的優位性を低下させていると評価しており、特に、中国、ロシア、北朝鮮、イランをあげている[1]。

1 中国

中国では、これまで、サイバー戦部隊は戦略支援部隊のもとに編成されていたとみられてきたが、この戦略支援部隊は、2024年に信息（情報）支援部隊などに再編された可能性が指摘されている。なお、2024年以前の戦略支援部隊は17万5,000人規模とされており、このうち、サイバー攻撃部隊は3万人との指摘もあった。台湾国防部は、サイバー領域における安全保障上の脅威として、中国が平時において、情報収集・情報窃取によりサイバー攻撃ポイントを把握し、有事では、国家の基幹インフラや情報システムの破壊、社会の動揺、秩序の混乱をもたらし、軍や政府の治安能力を破壊すると指摘している[2]。また、中国が2019年に発表した国防白書「新時代における中国の国防」において、軍によるサイバー空間における能力構築を加速させるとしているなど、軍のサイバー戦能力を強化していると考えられる。

参照 3章2節2項5（軍事態勢）

中国は、サイバー空間において、日常的に技術窃取や国外の敵対者の監視活動を実施しているとされ[3]、2023年には、次の事案への関与が指摘されている。

- 2023年4月、米司法省は、米居住の中国反体制派のオンライン会議において、反体制派の発信をメッセージの大量送信により妨害したとして、中国政府職員を起訴。
- 2023年5月、米国と英国などは、中国政府が支援するサイバーアクター「Volt Typhoon」が米国の重要

1 米国防省「サイバー戦略2023」（2023年）による。
2 台湾国防部「国防報告書」（2021年）による。
3 米国防省「サイバー戦略2023」（2023年）による。