2018 年 9 月 21 日

サイバーに関する安全保障上の課題

土屋大洋

1. 急所としてのサイバースペース

- サイバースペース＝通信端末＋通信回線（有線・無線）＋記憶装置＋データ
  - 設備から考えれば境界の確定は可能。データから考えるとわかりにくくなる。
  - 人工的に作られた空間であり、自然空間のアクター間の意思疎通を可能にする。
- サイバースペース≠インターネット:インターネットにはつながらないサイバーシステムの拡大。同じ技術が重要インフラストラクチャにも使われる。→サイバー攻撃の標的
- サイバースペースの 3D 化：深く（Deeper)、汚く（Dirtier)、暗く（Darker)。
  - 普通の検索エンジンでは表層しか見えない。
  - ダークウェブがサイバー犯罪やサイバー攻撃の温床に。
  - 無数に繋がる IoT（Internet of Things）端末の脆弱性とサプライチェーンリスク
- 物理的なインフラストラクチャの脆弱性：島国である日本は国際通信の 99%は海底ケーブルを経由。15 ヵ所の陸揚局（民間企業が所有）をどう守るか。ケーブルの切断は金融取引に即座に影響すると同時に、自衛隊の作戦活動に影響する。

2. 制空権・制海権から制脳権へ

- インターネット全体を破壊したい人は（サイバー犯罪者を含めて）ほとんどいない。しかし、ターゲットの指揮通信系（インターネットとは必ずしもつながっていない）を自身の都合の良いときに麻痺させたいと思っているアクターは多い。→サイバー戦だけでなく、情報戦、電子戦、電磁戦、ハイブリッド戦の可能性
- 拡大する作戦領域:陸、海、空、宇宙、サイバー空間、身体と脳（IoB: Internet of Bodies; Internet of Brains）→物理空間と情報空間、それがつながる人体・脳での戦いが視野に入りつつある。
- 他人の頭の中を操作する偽ニュース（大衆操作・プロパガンダが高度化し、容易に、安価に）→人工知能（AI）と同時に人間の頭脳の研究が進む。

3. 人工知能（AI）と自動化技術の採用

- OA 化、IT 化、デジタル化、オープン化、クラウド化……（バズワードは続く）
- AI は第三次ブーム：今回は本物だという人が多い（が……）。
- 民間資本による AI への投資は、投資家に富をさらに集中させ、社会を不安定化させる可能性（AI の呪い）

- 社会格差が大きく、人口が大きい国ではAIや自動化技術の普及が格差を固定化・拡大させ、ガバナンスを不安定にする可能性がある。
- 社会的格差が比較的小さく、人口が減少する日本では、うまく活用すればその恩恵はいっそう大きくなる可能性がある。

・ 軍事においては、兵器の「自動化」が戦局を変えてきた。
・ 今後も作戦活動における自動化技術の採用が進む。→最初にその効果が現れるのがサイバーセキュリティ（攻撃・防御）

4. 制脳権の時代の課題

・ 物理設備の防護：サイバー関連インフラストラクチャ防護の強化
- 自衛隊内の設備の電子戦・電磁戦対応
- 民間の電力供給網、海底ケーブル陸揚局、人工衛星基地局等防護の支援および演習
- 占用されている無線周波数の整理

・ 情報による安全保障：サイバーインテリジェンス活動の範囲と内容の見直し
- 平時と有事の境界が消失し、サイバー攻撃の有事判定は困難→いつ防衛出動させるか。
- オール・ドメインでのグレーゾーン事態への備え
- ハイブリッド戦に備えるためのオール・ソース分析の強化と部隊内連絡システム強化、隊員と家族の連絡態勢強化

・ 防衛・反撃能力の確保：サイバー防衛・反撃能力の研究
- クロスドメイン作戦への対応
  - 陸自、海自、空自の間の統合作戦
  - 日米間の統合作戦
  - 「例えば、陸軍が船を沈め、人工衛星を無力化し、ミサイルを打ち落とし、部隊を指揮統制する能力をハックしたり、妨害したりできなければならない。」（ハリー・ハリス米太平洋軍司令官）
- アトリビューション（攻撃者特定）能力が不可欠
- アクティブ・ディフェンスの検討：攻撃と防衛は表裏一体
- サイバー要員の増員とサイバー防衛隊司令の一佐から将への格上げ
- AI、自動化、IoB等の新技術採用