平和研所内会議

2010 年4月19日(月) 開催

テーマ:「安全保障空間の新たな地平−中国のサイバー攻撃と米国QDR 2010」

報告者:大澤 淳(主任研究員)

概要

1 2009 年12月半ばに、米国の Google 社は、中国を起源とする高度に洗練されたサイバー攻撃を受け、同社の知的財産が盗まれた、と発表を行い、中国政府との交渉の結果によっては、中国からの事業の撤退も辞さない姿勢を示した。

Google 社と中国側の交渉は1月中旬から3月中旬にかけて行われたが、3月22日、Google 社は、中国側との交渉が妥結に至らなかったとして、中国国内の検索サーバーを香港に移し、中国国内向けのサービスを続けると発表を行い、事実上中国本土から撤退した。

2 米議会の諮問機関である「米中経済安全保障検討委員会」は、2009 年 10 月 22 日に「中国のサイバー戦能力 (“Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation”)」に関する報告書を公表した。同報告書は、すでに公になっている中国の戦略関係の雑誌、新聞記事、西側の中国専門家へのインタビュー、実際のサイバー攻撃の事例など、中国国外で入手可能な公開情報を基に作成され、中国が戦略レベルでサイバー戦に力を入れていること、実際の西側へのサイバー攻撃が、金銭目的でなく、国防や外交政策などの特定の情報の詐取を計っていること、等を理由に、一連のサイバー攻撃は、中国政府が関与していると考えるのが、最も妥当であるとの結論を導いている。

3 上記の報告書によれば、後に人民解放軍参謀部第 4 部長(電子戦担当)となった戴清民少将が 1999 年に執筆した「情報戦入門」と題する、ネットワークと電子戦の複合的活用を提唱した本が出版されたが、これはその後中国人民解放軍に採用され、統合ネットワーク電子戦(「網電一体戦」)と呼ばれる戦略が現在採られている。「網電一体戦」は、敵が作戦を継続するのに必要な情報へのアクセスを拒否するため、敵のC4SIRネットワークと他の主要なネットワークに攻撃をかける戦略であり、中国人民解放軍は、戦時のみならず平時にもコンピュータ・ネットワークにおける特殊な役割を向上させている、と分析している。

4 上記の報告書は、有事の際の中国のコンピューターネットワーク作戦について、以下のように分析している。

4.1 有事においては、人民解放軍の司令官にとって、コンピューターネットワーク作戦は、ミサイルや空軍力と同様、戦闘の構成要素となる。

4.2 現在の人民解放軍の作戦戦闘要領においては、敵の結節点(node)を攻撃することで敵ネットワークを破壊し、通常の火力と合わせて敵の指揮命令系統および補給線を攻撃することが求められている。

4.3 この戦略は、米国のような高度な技術を持つ国に対して劣勢にある人民解放軍が通常兵力を用いて直接交戦を企図するよりも、戦いの初期段階において、人民解放軍が、コンピューターネットワーク作戦や電子戦を用いて敵の情報システムを攻撃する可能性があることを示している。

4.4 中国が米国との有事を迎えることになった際には、米国防総省のNIPRNET（Non-classified Internet Protocol Router Network)がターゲットになる可能性が高い。NIPRNETは米国の補給や指揮命令系統を補完しており、保秘のかからない情報をインターネット経由で受配信するシステムである。現在軍のグローバルな補給を支えるため、数百の民間･軍事ネットワーク結節点とつながっており、補給情報システムはこのNIPRNETに依存している。

4.5 また、台湾有事の際には、人民解放軍が直接優勢な米国と対峙することなく、米軍の来援を遅延させる手段として、コンピューター・ネットワーク作戦や電子戦を仕掛けてくる可能性が高いと考えられる。

5 米国内では、昨年の Google 社の発表と相前後して、中国からのサイバー攻撃に対する懸念が急速に増大してきており、このような懸念は、2010 年 2 月に発表された、米国防総省の 4 年ごとの国防政策見直し、QDR（Quadrennial Defense Review）2010 にも大きな影響を与えている。

6 QDR2010 では、複雑化する安全保障環境として、大きく以下の3点が指摘されている。

6.1 目下の紛争：イラク、アフガニスタン、アルカイダおよびその同盟者との戦いは、今後数十年間の安全保障環境を形作る。

6.2 長期的な傾向として、①新興国の台頭、②非国家主体の伸張、③WMD および弾道弾ミサイルを含む危険な技術の拡散、④資源の枯渇、気候変動、新型疾患、人口動態、の4点が複雑化する安全保障環境を作りつつある。

6.3 今後米国が直面する作戦環境上の課題として、①「ハイブリッド脅威」とも言うべき、多次元の紛争の発生、②グローバルコモンに対する脅威の出現（特に宇宙およびサイバー空間）、③潜在的に敵対する可能性のある国による「介入阻止」能力の増大および弾道弾ミサイル脅威の増加、④破綻国家／不安定国家の増大、の4点が脅威として浮上してくる。

とくに、6.3②の「グローバルコモンに対する脅威」は、具体的に上記の「米中経済

安全保障検討委員会」指摘している懸念が念頭にあると見られる。

7　そのような安全保障環境の分析を受けて、特に 6.3②の「グローバルコモンに対する脅威」および 6.3③潜在的に敵対する可能性のある国による「介入阻止」能力の増大、という中国を念頭に置いた脅威に対しては、介入阻止環境において侵略を抑止・打破できるよう、以下のように、米国は軍事力バランスを見直すとしている。

7.1　米国は敵対する可能性のある国による侵略を抑止／打破する。そのような国が「介入阻止」能力を持っている場合でも、米軍の戦力展開を確保できるようにする。具体的には、長距離攻撃力の拡大、水中作戦での優位性の確保、米国の前方展開と基地インフラの増強、宇宙空間へのアクセスと宇宙資産利用の確保、諜報／監視／偵察能力の強化、敵の早期警戒システムおよび交戦システムの打破、海外にいる米軍のプレゼンスと対応力の強化を行う。

7.2　サイバー空間における脅威に対抗する能力の向上が求められている。21世紀においては、サイバー空間へのアクセスと信頼性のある情報コミュニケーションなくして、軍事行動を行う事は出来ない。国防省の情報ネットワークは、接近阻止戦略を持ち、米軍の展開を遅らせようとする敵国の標的になっている。このような外国の情報機関や軍は、米国の軍事能力の機能を妨害しようとして、国防省のネットワークの改ざんをはかっている。このような外国からのコンピュータ・ネットワーク攻撃に対して、有効な防御策を講じなければならない。米国は、サイバー空間における作戦行動の包括的アプローチの開発、サイバー領域の脅威と脆弱性に関する専門知識の向上、サイバー部隊の強化、他国とのパートナーの強化を行う。

8　中国の「網電一体戦」戦略に於いて、中国は、自国のどのレベルのサイバー攻撃が「戦争」を意味するのか明確に定義をしていない。また、より大きな紛争を避けるために小さな戦争を戦うことを抑止の概念に含めているため、血の流れないサイバー攻撃や電子戦を、危機をエスカレートさせないために利用可能な抑止の手段と認識している可能性がある。中国政府が、サイバー攻撃が敵の「レッドライン」を超えないと判断した場合には、これらの攻撃を大きな紛争を抑止するために積極的に利用することも考えられる。

9　しかしながら、米国側のサイバー攻撃に対する認識は、サイバー攻撃＝戦争である。中国が大きな紛争を抑止しようとして有事の際にサイバー攻撃を行った場合、米国がこれを「全面的な戦争」と認識する可能性も考えられる。国際政治の歴史を振り返ると、この種の「誤解」「誤認識」によって、戦争が発生した例は枚挙にいとまがない。今後、「グローバル・コモン」における、コンピューター・ネットワーク作戦や電子戦の危険性について、国際社会で議論を深め、共通感覚（common sense）を形成する必要がある。

以上