中国軍がハッカー部隊を強化

漢和防務評論 20151201 (抄訳)

阿部信行

（訳者コメント）

中国軍は、ハッカー部隊を強化しつつあります。
中国軍のハッカー部隊構成員は、コンピューター技術に精通した者たちの中から選抜された要員ですが、民間の技術者も活用しています。民間人の彼らは、政府のコントロールの下にはなく、外国政府機関のホームページに侵入したり様々な事件を起こしているのは彼らであると考えられます。
数年前、中国ハッカーの犯行が明らかになった際、政府機関は関与を完全否定しましたが、中国の専門家は、ネット上の記事で、”君たちの愛国精神は理解できるが、政府に迷惑をかけるのは良くない”との趣旨を述べていました。
習近平が関与を完全否定するのは、軍人が関与していないことを主張しているだけであると思います。民間人の犯罪行動までは関与できないということでしょうか。

KDR ニュース平可夫特電：
中国軍は、陸海空軍及び第二砲兵部隊内に建設されたネット攻撃及び防御を専門とする”紅客”（黒客）部隊（註：ハッカー部隊を指す）を強化している。中国政府は、ハッカー部隊の存在を正式には認めていないがその兆候が顕著に見られる。
"HACKER"の中国語訳は、”黒客”である。”黒”は中国文化の中で評判の悪い言葉に使われる。したがって中国軍内部では、黒客部隊を”紅客”に変更している。総参謀部 3 部及び 4 部にネットワーク戦専門の部門がある。ネット攻撃の最高位担当部門は、総参謀部情報化部である。陸軍は、軍級単位に情報化担当部局を設け、情報戦分隊を隷属させ、”紅客”に専らネット攻撃を実施させている。
中国軍は、ネットワーク戦部隊を進攻部門と防護部門に区分している。”紅客”部隊は前者である。
総参謀部は、情報化部内に”情報安全局”を設立し、進攻と防護を担当させている。”総参謀部直属の情報作戦力”と称される同部門には、全軍から最も優れたハッカー専門家を集め、各種のウィルスを研究開発させ、ネット進攻に利用している。少なくとも 7 個の工房、1 個の研究所、1 個の支援基地を保有し、コンピュータウィルスの開発と生産を行っている。
情報作戦局の主要な使命は、ネット情報の偵察であり、主として敵の戦略及び戦役にかかわる情報系統の構成と運用の特徴、敵情報戦力の編成、部署及び行動計画を探ることにある。また諸軍兵種の中に戦役ネット情報戦戦力を配置し、敵の重要戦略、戦役ネット情報、及びネット情報系統に対して電子攻撃及びネット攻撃を行う。

さらにその他の作戦戦力と協同して戦役情報防御を行う。さらにまた味方のネットワーク情報系統の保全を図り、味方情報系統の効果を正常に発揮させる。
4 つの軍種には、それぞれ独立作戦及び協同作戦を行うネットワーク作戦大隊及び分隊が組織されている。それらは司令部及び艦隊所属の情報化担当部門に直属している。第二砲兵は、この方面の技術研究が相当進んでいる。第二砲兵のネットワーク情報作戦戦力の主要任務は、ネットワーク情報進攻、欺編、及びネット防御であり、米国の ICBM 部隊のネットワーク情報系統の破壊するとともに、第二砲兵のネットワーク情報系統を保護し、系統の効果を正常に発揮させることである。またその他の軍兵種のネットワーク戦力と協力し、共同して局地の制情報権を奪取する。集団軍は、情報化担当部門として情報戦大隊を設立し、ネットワーク進攻と防御を行っている。ほぼ全ての軍兵種について、ハッカー部隊の作戦の段取りは以下の通りである：

1. ネット偵察を行う。主として有線及び無線によるアクセスを総合運用することにより、敵ネットワークの通信体制、モデム方式、ネットプロトコル、操作系統の特徴及び脆弱性の分布等を重点的に調査し、ネットワーク攻防のための情報を提供する。
2. ネットをスキャンし探知活動を行う。目標とする敵ネットワークに対してスキャンし、分析し、敵ネットワーク系統の位相構造、ネットプロトコル、ホスト名、IP アドレス、操作系統等の情報を広範に収集し、敵ネットワークのセキュリティホールと弱点を捜索し、ネット攻撃のための目標と突破口を探知する。
3. 各種の手段を用いて、敵のネットワークに進入し、盗聴装置を仕掛け、敵ネット上に流れるデータを入手し、ユーザーパスワード、作戦電文、ルーター等の価値ある情報を入手する。
4. 敵指揮所ゲートウェイ、メインルーター、ネット管理センター等の要害及び核心部分にネット盗聴器を仕掛け、敵の重要なユーザーのアドレス、パスワード、通信流量を探知し、その上で敵の指揮体系、兵力部署、作戦行動等の重要情報を解析する。
5. ネット上で敵の秘密を窃取する。これは、敵のネット上に保存され、伝送され、コピーされた秘密情報を窃取することである。
6. 目標とする敵のネットに嵌めこみ或いは特定の”トロイの木馬”を駐留させ、目標とするホストコンピューターを遠隔操作し或いは予め自動設定した特定の操作を実施させる。またこれを踏み台にしてその他のホストコンピューターを攻撃する。
7. 味方のコンピューター資源を利用し、敵のネットに大量にアクセスし、情報を無効にし、目標とする敵ネットワーク及びホストコンピューター、或いはサーバーの正常な機能を無効にする。
8. 敵のホストコンピューター或いはサーバーに存在するセキュリティホール或いは予め残置した”後門（不正なソフト)”を利用し、敵のホストコンピューターに秘密の指令を送り、ユーザー特権を偽造し、目標とするシステムを停止させ、シス

テムの時刻補正を応用しサーバー及びデータバンクを自由に操作する。
9. 敵の情報ネットワークにウィルスを送り、敵システムのハード及びソフト或いは情報資源を破壊する。或いは多種類の技術手段を総合的に利用し、敵のネット上の通信系統を遮断し、敵ネット上のサーバーを麻痺させる。
10. 電磁妨害手段を利用し、ネット環境及びネット設備に電磁妨害を行う。そして敵の磁気記録中のデータを破壊し、また敵が使用中の電源及び帯電設備に衝撃を与える。
11. ウィルス攻撃を行って汚染を拡大させる。長期にわたってウィルスを潜伏させ、予定時期に破壊する。
12. 敵の暗号を解読する。敵の情報の結節点に向けて大量のデータを送り、情報処理資源を消耗させ、ネットを閉塞させる。
13. ネット上のハードウェアを破壊する。ハードウェアに対する”地雷”攻撃を行う。”地雷”は、予めハードウェア中に設けられた特殊な電気回路である。ハードディスクを破壊するマイクロロボット或いはハードディスクに対する細菌攻撃である。

中国軍は、”ハッカー”を養成するに当たり、民間のコンピュータ技術者を十分に利用している。利用できるすべての情報手段を使用しようとするならば、民衆のネット技術力を活用し、ネット情報で部隊を支援してくれる人材グループを建設する必要がある。さらにネット民兵を組織しようとするならば、”ネット人民戦争”を発動しなければならない。
近年来、多くの NATO 国家、日本政府、経済、及び金融機関のネットが攻撃されている。日本では、今年、防衛省管轄のホテル（主として自衛隊の来訪者を接待する）のネットが侵入され顧客のデータが盗まれる事件があった。多くの国家の政府は、これらのネット犯罪は中国と関係があると述べている。しかし中国は徹底否認している。

以上