ＢＳＫ第２２－５号

中華人民共和国のサイバー戦とコンピュータ・ネットワーク・エクスプロイテーション能力

―（米中経済安全保障調査委員会への提出資料）―

米中経済安全保障調査委員会議会報告２００９から抜粋

第２章：合衆国の安全保障利益に直接影響を及ぼす中国の活動

第３節：合衆国を攻撃目標とした中国の人的スパイ活動と合衆国国家安全保障に及ぼす影響

第４節：合衆国を攻撃目標とした中国のサイバー活動と合衆国国家安全保障に及ぼす影響

平成２２年９月

財団法人 防衛調達基盤整備協会 ®

はしがき

２００９年７月、米国及び韓国の政府機関等のウェブサイトが大規模なサイバー攻撃を受けたが、このことは、経済活動や社会生活の多くの面において情報通信技術への依存が進む我が国にとっても、情報セキュリティ上の脅威が安全保障・危機管理上の問題となり得ることを示すこととなった。

折しも、同年１０月に出版された米中経済安全保障調査委員会の年次報告は、４章構成の約４００頁に及ぶものであるが、第２章で「合衆国の安全保障利益に直接影響を及ぼす中国の活動」について記述している。

特に、同章第３節「合衆国を攻撃目標とした中国の人的スパイ活動と合衆国国家安全保障に及ぼす影響」及び第４節「合衆国を攻撃目標とした中国のサイバー活動と合衆国国家安全保障に及ぼす影響」を取り上げ翻訳するとともに、この第４節の報告に当って参考資料とした民間会社との調査研究委託による「中華人民共和国のサイバー戦とコンピュータ・ネットワーク・エクスプロイテーション能力」も合わせて公表されているので、翻訳したものである。

これら３件の資料は、中国の経済及び軍事面におけるインテリジェンス活動の増大、とりわけサイバースペースを利用した活動が活発化していることとそれらの活動が何らかの国家的関与を示していることを明らかにしている。

また、中国の経済及び軍事の近代化のため、情報通信技術の導入を積極的に推進している実態やサイバー戦に対する戦略は、米国を正面に見据えて、民兵組織を含めた訓練を行うなど、その態勢作りにまい進している様子が明らかにされている。

このような米中間のサイバースペースの出来事及び中国のサイバー戦戦略は、我が国にとっても注視すべきものと考える。

これら３件の資料を翻訳した出版物が、我が国における技術情報管理の向上にいささかでも貢献できれば、望外の幸せである。

平成 22 年９月

財団法人　防衛調達基盤整備協会
理事長　宇田川　新一

中華人民共和国のサイバー戦と
コンピュータ・ネットワーク・エクスプロイテーション能力

（米中経済安全保障調査委員会への提出資料）

提出資料

プロジェクト・マネージャ
Steve DeWeese 703.556.1086 steve.dweese@ng.com

筆頭著者
Bryan Krekel

主題専門家
George Bakos
Christopher Barnett

ノースロップ・グラマン社
情報システム部門
7575 Colshire Drive
Mclean, VA 22102

2009年10月9日

NORTHROP GRUMMAN

目　次

記述範囲

本報告書は、中国の平時及び紛争時におけるコンピュータ・ネットワーク作戦(Computer Network Operation: CNO)の遂行能力評価を、広範なオープン・ソースに基づいて行ったものである。本報告書に示す調査結果が、政策立案者、中国専門家及び情報作戦専門家にとって有用な参考資料となることを期待する。本プロジェクトは、中華人民共和国(People's Republic of China: PRC)が CNO を如何に着実に進めているか、及びその履行状況はどの程度なのかを明らかにするため、次に示す 5 つの広範囲に及ぶ分類に従って調査を行なったものである。

(1) 中国人民解放軍(People's Liberation Army: PLA)の軍事行動及び戦略レベルにおける CNO 戦略。これは、中国がこの能力をどのように全体の計画立案活動に統合しているか、及び戦闘部隊においてどのように運用できるようにしているのかを理解させるものである。
(2) 中国の CNO における主たる制度上及び個々の「行為者」は誰か、並びに軍及び民のオペレータ間に存在するつながりは何か。
(3) 紛争時における中国の対合衆国 CNO 攻撃目標の候補。これは、紛争時における PLA の合衆国又は同様の技術的先進軍隊に対する情報管理奪取の企てがどのようなものかを理解するためである。
(4) 合衆国政府及び民間セクターを攻撃目標とした現在のネットワーク・エクスプロイテーション活動の特徴。これらの活動は、しばしば中国の関与があるとされている。
(5) 中国による合衆国政府及び企業ネットワークへの侵入活動とされる歴史年表。これは、その広範な活動情況を示すものである。

本報告書は、信頼できるオープン・ソース対する厳密な調査に基づいて実施したものである。それらのオープン・ソースは、PLA の文書、西側の PLA や情報戦アナリストに対するインタビュー、これら問題に関連した西側の研究成果、及び中国が発生源と判断された合衆国ネットワークへの侵入に対するフォレンジック分析であり、とりわけ、中国国防大学や軍事科学大学が出版した記事や論文からの情報に重点を置いた。これらの大学は、軍におけるドクトリン、戦略及び軍の近代化に係る出版物に関して最も権威がある。これらの出版物のほとんどは、中国の情報戦(Information Warfare: IW)及び CNO に係る戦略及びドクトリン上の問題に対する現在の考え方について、かなりの識見を示している。より広範な軍事行動ドクトリン及び戦略における IW の役割に係る識見については、「軍事戦略科学(The Science of Military Strategy)」及び「軍事行動科学(The Science of Campaign)」から入手した。これらは、オープン・ソースにおいて入手できる最も権威ある情報源である。IW 訓練に関するデータについては、軍の公式新聞である「人民解放軍

日報」、並びに中国軍事記事、公式メディア及び非中華人民共和国地域のメディアだけでなく中国の省や地方のメディア提供記事から入手した。

中国が関与した侵入によく見られたスパイ活動手順に対する技術評価は、詳細なフォレンジック分析及びこれら問題を注視する情報セキュリティ専門家との検討結果によるものである。また、本調査においては、CNO 及びエクスプロイテーション[1]技術に係る中国技術雑誌の論文も参考とした。これらの論文は、合衆国でオンライン・アクセスが可能な中国関連データベースから入手したものである。

中国のハッカー・ウェブサイトに掲載されている内容及び議論に係る調査は、これらハッカー・グループの活動及び能力を分析する際の参考となった。この調査の焦点は、これらグループと政府間の関連の有無を明らかにすることであった。本調査の焦点をどこに当てるかに当たり、これらのグループや活動家に注目している西側の情報セキュリティ分析家との対談は大いに参考となったばかりでなく、我々の中国ハッカー・コミュニティに関する理解を深めるのに大いに役立った。

本調査範囲には、中国内における調査は含まれていない。したがって、著者達は、中国外で現在入手可能な資料及び識見に焦点を当てて調査を行った。本論題に関連した中国内におけるさらなる調査は将来の達成努力方法であり、それによって本調査結果を補完することができ、またそうすべきである。

---

[1] 訳注：エクスプロイテーション：英語表現は「exploitation」であり、開拓、開発、利用、活用、利己的利用、搾取などの意味がある。サイバー・セキュリティの用語としては、利己的利用や搾取に近い意味を持たせており、エクスプロイト・コードなどにより、セキュリティ・ホールの存在を確認することをいう。そして、この結果を攻撃ツールに利用して、標的を攻撃することになる。したがって、単に「利用」又は「悪用」と翻訳することは適切でないと考えられることから、本訳文においては、「エクスプロイテーション(名詞)」及び「エクスプロイト(動詞)」の用語を利用した。なお、中国軍が利用しているコンピュータ・ネットワーク・エクスプロイテーション(Computer Network Exploitation: CNE)の用語は無論のこと、コンピュータ・ネットワーク作戦(Computer Network Operations: CNO)、コンピュータ・ネットワーク攻撃(Computer Network Attack: CNA)及びコンピュータ・ネットワーク防衛(Computer Network Defense: CND)の用語のすべては、次に示す米国防総省の用語の意味に同じである。

- ✧ CNO：コンピュータ・ネットワーク攻撃、コンピュータ・ネットワーク防衛及びコンピュータ・ネットワーク・エクスプロイテーションから構成される。
- ✧ CNE：コンピュータ・ネットワークを利用し、攻撃目標又は敵対者の自動情報システム又はネットワークからデータを集めることによって実施されるインテリジェンス収集活動をいう。
- ✧ CNA：コンピュータ・ネットワークを利用し、コンピュータとコンピュータ・ネットワーク内の情報又はコンピュータとネットワークそれ自身を混乱、妨害、機能低下又は破壊するための活動をいう。
- ✧ CND：国防総省情報システム及びコンピュータ・ネットワーク内において、認可されていない活動を防止、監視、分析、検知及び対応を行うための活動をいう。

管理者向け要約

中華人民共和国(PRC)政府はここ十年間、ハイテク戦争における戦闘能力確保への根本的な転換を目指し、徹底的な軍近代化プログラムを推進している。中国軍は、全戦闘部隊及び全指揮階層において通信可能なネットワーク化された部隊をますます増加させ、従来の台湾に焦点を当てた任務をはるかに超えたより地域的な防衛態勢へと推し進めている。この近代化活動は、情報化(informationization)として知られているが、戦闘ドクトリン「情報化された環境下における局地戦争(Local War Under Informationized Condition)」によってその方針が示されている。このドクトリンは、陸海空及び宇宙における軍事作戦と全電磁スペクトラムの調整能力を備えた完全にネットワーク化されたアーキテクチャーの開発を目指す現 PLA の活動に言及している。

このドクトリンの焦点は、先進 IW 能力の開発促進に当てられている。そして、その明らかにされた目標は、戦場において敵対者の情報の流れをコントロールするとともに、味方の情報の流れを維持することとしている。中国の軍事戦略家は、戦闘全般における成功を獲得するための備えとして、ますます情報優勢に注目している。また、中国人民解放軍(PLA)の IW に対する重要性の高まりは、より包括的なコンピュータ・ネットワーク・エクスプロイテーション(Computer Network Exploitation: CNE)技術の開発へと走らせている。この CNE は、戦略的なインテリジェンス収集目的を支援し、潜在的な将来の紛争における成功の礎となるものである。

PLA における情報化プロセスを促進させる主要戦略の一つは、CNO、電子戦(Electronic Warfare: EW)及び敵のネットワーク化された情報システムを攻撃する運動エネルギー兵器の組み合わせを利用するものである。様々な PLA 部隊が、この組み合わせを利用することによって、予め計画した時に又は戦術状況が是認する場合に、利用可能な「盲点(blind spot。通信が困難な地域)」を造りだすことができる。敵対者のインテリジェンス、捜索及び偵察(Intelligence, Surveillance and Reconnaissance: ISR)システムなどの重要標的への攻撃は、ますます洗練されたジャミング・システムや対衛星(Anti-Satellite: ASAT)兵器が配備された EW 部隊及びカウンタースペース部隊の任務である。敵対者のデータ及びネットワークに対する攻撃は、コンピュータ・ネットワーク攻撃(Computer Network Attack: CNA)及びエクスプロイテーション(CNE)専門部隊の任務であると判断される。

中国には「統合ネットワーク電子戦(Integrated Network Electronic Warfare: INEW)」と題する公式 IW 戦略がある。これによれば、PLA の総参謀部(General Staff Department: GSD)第四部（対電子戦）[2]下にある CNA と EW 両者の攻撃任務を統合する一方、コンピ

[2] 総参謀部は、PLA における最上位の組織であり、軍事に係る日常管理任務を遂行している。総参謀部は 7 つの職務部から構成されている：作戦、インテリジェンス、信号インテリジェンス、対電子戦、通信、

ュータ・ネットワーク防衛(Computer Network Defense: CND)とインテリジェンス収集任務を GSD 第三部（信号インテリジェンス）の隷下に、そしておそらくは PLA の様々な IW 専門の民兵部隊に置いているようである。

この INEW 戦略は、敵対者の指揮・統制・通信・コンピュータ・インテリジェンス・捜索及び偵察（Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance: C4ISR)ネットワークやその他の重要な情報システムに対する EW と CNO の同時適用に依存しており、これが中国の攻撃的 IW の基礎と思われる。この戦略の分析結果は、紛争時の早期段階において CNO ツールが広く採用されること、そしておそらくは敵の情報システムと C4ISR に対する先制攻撃として実施されることを示唆している。

PLA は、部隊における様々な IW ツールの利用を促進するため、その装備化と訓練を行っており、これにより紛争間における敵対者への情報優勢を確立しようとしている。PLA の攻撃ドクトリンは、紛争時における作戦の最優先事項の一つとして、敵対者に対する情報優勢の早期確立を明確なものとしていることから、INEW 戦略がこの目的に沿ったものと考えられる。

PLA は、IW 能力の速やかな成長に必要される急激な人的資源増を満足させるため、中国の広範囲に及ぶ民間セクターに適任者獲得の手を伸ばしている。それらの人物には、民間企業、大学、そしておそらくは中国の選ばれたハッカー・コミュニティからの専門スキルを持った者が含まれる。PLA と中国のハッカー・コミュニティ間の固い結束を示す証拠は、オープン・ソースにほとんど見ることができない。しかしながら、調査の結果、よりえり抜きのハッカーと中国公安部との間の明白な協同関係を示すいくつかの事例が明らかとなった。ただし、詳細さの点で限界があり、ハッカー・コミュニティと PLA や中国との関係を確証するのが困難であったことに留意されたい。

中国は、その成熟した CNE 能力を利用して合衆国政府と企業に対する洗練された CNE 攻撃を長期にわたり実施し、これによりインテリジェンス収集活動を支援しているようである。このインテリジェンス収集支援活動に係る問題は、中国の統制のとれた標準運用手順、洗練された技法、高級なソフトウェア開発資源へのアクセス、攻撃目標ネットワークに対する深い知識、及び時には数ヶ月にも及ぶ攻撃目標ネットワーク内での CNE 活動の維持能力である。

これら侵入の分析結果からは、それらの侵入者がますます中国の「ブラック・ハット」

動員、外事及び管理。

プログラマー(すなわち、不正なハッキング活動を支援する人物)に変わっているとした証拠を明らかにしている。彼らは、カスタマイズ・ツールを利用し、ベンダーが未発見のソフトウェアぜい弱性を利用している。この種の攻撃は「ゼロデイ・エクスプロイト又はゼロデイ(zero day exploit or 0-day)」として知られている。これは、防御側がぜい弱性情報発表からの日数を数える前に(ぜい弱性情報が公表される前に)、攻撃されることを意味するものである。もっとも、これらの関係が何らかの政府関与を証明するものではないが、現在合衆国ネットワークへの侵入に加わっている人物は、中国語に堪能で、中国の地下ハッカー・コミュニティとの固い結びつきを持っていることは確かである。さもなければ、合衆国ネットワークを標的にしている人物は、中国のブラックハット・ハッカー・コミュニティとの関係を維持し、攻撃中においても攻撃ツールに対する展開支援を受けられるインフラにアクセスすることが可能な潤沢な資源を持っていることを暗示するものである。

合衆国や世界中の多くの国々を標的にした CNE 活動範囲の維持に必要となる専門知識供給源の深さは、その標的が防衛用エンジニアリング・データ、合衆国軍事作戦情報及び中国関連政策情報に極めて集中していることから、サイバー犯罪組織の能力や側面をはるかに超えるものであり、少なくともある種の国家的支援関係がないと困難である。

一般的に、密かに盗む目的で攻撃目標にされる情報の種類は、サイバー犯罪におけるクレジット・カード番号や銀行口座情報などと異なり、金銭的価値が本質的にないものである。仮に、盗まれた情報が第三者によって関心を持つ国に仲介されたとしても、また実際にキーボード操作を行なっている人物の所属がどこであろうとも、その活動は技術的に見て「国家的支援」を受けていると考えられる。

今日まで攻撃目標とされてきた合衆国の情報は、国家の防衛企業、宇宙プログラム、選定された民間ハイテク企業、合衆国の主要な中国問題に係るリーダーシップの考えに関心を抱く政策立案者、並びに危機の間に利用可能な合衆国の防衛ネットワークや兵站及び関連する軍事能力のインテリジェンス事情を把握する対外軍事立案者を利する可能性を秘めている。攻撃目標範囲の広さ及びこのデータに対する潜在的「顧客」の範囲は、インテリジェンスを収集し管理するインフラの存在、又は実行中の活動範囲を、時にはほぼ同時に、効果的に統制する監督機関の存在を示唆している。

中国が、合衆国との紛争の間に、軍の非秘密区分指定インターネット・プロトコル・ルーター・ネットワーク(Non-classified Internet Protocol Router Network: NIPRNET)及び合衆国本土とアジア太平洋地域の同盟国に設置してある国防総省と民間契約者の兵站ネットワークの選定ノードを攻撃するため、その CNO 能力を利用することはほぼ確実と思われる。中国のこれらシステムに対する標的行為は、合衆国の部隊展開遅延をもたらし、戦

場に展開している部隊の戦闘能力の効果性に影響を及ぼすことが目標である、と中国は明言している。

PLA の敵対者に対する CNO の適用に際しての具体的基準、又は中国の指導者がどのような種類の CNO 行動が戦争行為を構成すると信じているのかについては、これを明示した信頼できる PLA オープン・ソース文書はない。

結局のところ、CNE と CNA の唯一の違いは、キーボードにタッチしているオペレータの意図の違いということになる。平時におけるインテリジェンス収集目的のネットワーク侵入に必要なスキル・セットは、有事における攻撃活動目的のネットワーク侵入に必要なスキル・セットと同じである。その違いは、キーボードにタッチしているオペレータが、いったん標的にしたネットワークに侵入したときに、情報に対して何を行うかということである。仮に、中国のオペレータが、合衆国政府及び民間ネットワークを標的にし、現在行っているエクスプロイテーション活動のいくつかは自分によるものであると確かに思うのであれば、彼らは既に運用上十分熟達した CNO 能力者であることを示したことになる。

1　中国のコンピュータ・ネットワーク作戦戦略

中国人民解放軍(PLA)は、積極的にコンピュータ・ネットワーク作戦(CNO)の能力開発を行うとともに、在来戦闘分野の支援に必要な戦略的ガイダンスやツールの策定及び訓練を実施している。にもかかわらず、PLA は、ドクトリンや戦略策定の主要組織体である中国の最高軍事意思決定組織体としての中央軍事委員会(Central Military Commission: CMC)又は軍事科学院(Academy of Military Science: AMS)の公式審査に基づく CNO 戦略の出版を公にしていない。しかしながら、PLA は「統合ネットワーク電子戦(INEW)」と題する戦略を策定し、CNO 及び関連する情報戦ツールの利用ガイダンスを提供している。この INEW 戦略の特徴は、ネットワーク戦ツールと電子戦兵器の併用により、紛争の早期段階において敵対者の情報システムに対抗するとしていることである。

中国の情報戦戦略は、PLA の情報化環境における局地戦戦闘ドクトリンと密接な吻合が図られており、現在のドクトリンは、陸・海・空・宇宙及び全電磁スペクトラムにおける軍事作戦一元化能力をもつ完全なネットワーク・アーキテクチャの開発を求めている。中国軍は、大規模な陸軍に依存した毛沢東時代の人民戦争からシフトしており、先進の C4ISR 技術でリンクされ、完全に機械化された軍へとなりつつある。

情報化は、本質的にはハイブリッドの開発プロセスであり、機甲化傾向を継続しつつ現在の軍事組織のほとんどを維持する一方で、それら組織に完全にネットワーク化された指揮統制(C2)インフラ[3]を構築するための先進情報システムを重ねるものである。この構想は、PLA が現在の取得戦略又は戦力組成を急激に変更することなく、既存の軍事組織のネットワーク化を可能にしている。

- ✧　現在及び将来の戦闘に対する PLA のアセスメントは、陸・海・空・電磁のすべての領域において軍事行動が同時に行われることを言及している。しかし、特にその焦点となっているのは後者(電磁)の領域であり、これが PLA による情報化環境ドクトリン[4](Informationized Conditions doctrine)の採用を促進させている。

また、このドクトリンは PLA の軍事行動アプローチの方法にも影響を与えており、従来からの戦闘部隊連合作戦から PLA の言う「情報化環境における統合連帯作戦」へのシ

---

[3] 中国の国家防衛2008、中華人民共和国・国務院情報室、北京、2008年12月29日、
http://www.chinadaily.com.cn/china/2009-01/20/content_74133294.htm
[4]中国の国家防衛2004、中華人民共和国・国務院情報室、北京、2004年12月27日、
http://english.peopledaily.com.cn/whitepaper/defense2004/defense2004.html。中国の国家防衛2006、中華人民共和国・国務院情報室、北京、2006年12月29日、
http://english.chinamil.com.cn/site2/newschannels/2006-12/29/content_691844.htm

フトを企てている。前者は、大規模な機甲化された縦列戦闘隊形ながら、共通の運用画面(common operating picture)の共有がないことに特徴付けられる。そして後者は、陸・海・空・宇宙を一つの多次元戦場に適合させるため、情報技術の優勢とその能力を強調するものである。PLA は、統合連帯作戦の枠組みにおいて、軍務と戦闘規律を全体として一つの統合作戦に結び付けて考えるため、情報ネットワーク技術を利用するとしている。これも、PLA の情報戦へのアプローチを具体化するものでもある。

PLA の軍事作戦ドクトリンに関し、最も権威のある公的声明とされている軍事戦略科学と軍事行動科学の 2 件は、情報優勢の獲得が PLA の戦略的及び軍事行動レベルにおける主要な目標であると述べている[5]。敵対者の情報フロー管理を制圧し、情報優勢を獲得することは、PLA の軍事行動戦略における不可欠な要求事項であり、「軍事戦略科学」がそれらを空及び海の優勢を奪取するために必要不可欠と考えている根本的基礎になっているものと考えられる[6]。

- ✧ 「軍事戦略科学」と「軍事行動科学」の両者とも、敵の C4ISR 及び兵站システム・ネットワークを IW 攻撃の最優先順位として明らかにしている。これは、紛争間における合衆国やその他の技術先進対抗勢力に対する標的を決定するに当たって、その指針を与えるものと思われる。
- ✧ 「軍事行動科学」は、IW が軍事行動の開始を示さねばならず、適切に利用することによって全作戦の成功を可能にする、と明言している[7]。

部隊の機甲化から情報化への移行に対する緊急性の気配は、最初に敵の情報アクセスを抑制する強力な IW 能力がなければ、合衆国など大きな技術的優勢を持つ敵対者に局地戦において勝利するのは不可能であるとした認識にかられたものと思われる[8]。

- ✧ PLA の情報優勢に係る議論は、敵対者の C4ISR インフラ攻撃に焦点を当てており、同インフラによる意思決定又は戦闘作戦を支援する情報の取得、処理や伝送を抑止又は中断させることとしている。その目標は、ミサイル、空爆、又は軍事施設やハードウェアに対する特殊部隊の投入を利用した適切なハードキル選択肢の組み合わせによって攻撃を行い、敵対者の指揮・統制アーキテクチャーの機能を麻痺

---

5 主編纂者 Wang Houquig 及び Zhang Xingye、「軍事行動科学」、北京、国家防衛大学出版社、2000 年 5 月。第 6 章第 1 節軍事行動場面における情報戦の外観を参照。Peng Guanqgiang 及び Yao Youzhi 共著、「軍事戦略科学」、軍事科学出版社、英語版、2005 年

6 Peng と Yao、338 ページ

7 OSC、CPP20010125000044、「軍事行動科学、第 6 章、第 1 節」、2000 年 5 月 1 日

8 OSC、CPP20081112563002、「情報化環境における作戦理論の変化動向」、Li Zhilin 著、中国軍事科学、2008 年冬。OSC、CPP20081028682007、「情報戦における考察モードの基本的特性の研究」、Li Deyi 著、中国軍事科学、2007 年冬

させることである。

- ✧ これらのネットワーク機能の低下により、敵の情報の収集、処理及び伝達、又は戦闘作戦の支援に必要な情報へのアクセスを妨げることが可能である。これにより、台湾海峡シナリオにおける合衆国の効果的な介入前に、PLA 部隊の台湾上陸などの作戦目標を達成することができる。

また、PLA は、真の情報優勢を達成する手段として、宇宙ベースの情報資産を抑制する重要性を認識するようになっており、それを「新戦略的重要問題(new strategic high ground)」と呼んでいる。そして、その支持者の多くが、宇宙戦を情報戦の部分集合として考えている[9]。PLA は、宇宙を利用した軍事作戦機能の開発に努めているが、一方で同じ機能を敵対者がもつことを拒否している。また、PLA の著者は、連帯軍事行動作戦と戦場におけるイニシアティブの維持に、宇宙優勢が不可欠であることも認識している。逆に言えば、彼らの意見は、敵対者の宇宙システムに対する拒否が情報戦に不可欠な要素であり、かつ、勝利に不可欠であるということになる[10]。

PLA は、強力な研究開発の焦点をカウンタースペース(counterspace)兵器に当てている。現在開発中の多くの能力はサイバー又は EW の選択肢を全く超えたものであるにもかかわらず、彼らは未だに「情報戦」兵器であると見なしている[11]。中国の衛星攻撃兵器(Anti Satellite Weapon: ASAT)能力で最も目立つのは運動兵器であり、人工衛星に直接衝突させるための高速度で発射された発射物又は弾頭によるものである。2007 年 1 月に行われたこの能力のテストは、機能停止状態の中国の気象衛星に対して行われ、成功した。これは、PLA がこの選択肢に係る過去の理論的論議から、運用能力の確保に向けて移行したことを示すものである。レーザー、高出力電磁システムや核爆発(nuclear generated)電磁パルス攻撃(Electro Magnetic Pulse: EMP)などの指向性エネルギー兵器については、現在開発中である。これらに認められる利点は、即時性、及び EMP の場合はその効果範囲が大きいことである[12]。

これらの兵器のいずれかを合衆国の人工衛星に対して利用することで危機が急激に拡大すると同時に、たとえその攻撃が上空の大気圏で行われるにせよ、EMP 効果を引き起こ

---

9 Dean Cheng 著、「宇宙に対する PLA の見解：情報優勢に不可欠」、海軍分析センター、CME D0016978.A1、2007 年 10 月、7 頁

10 情報戦に不可欠な統合空・宇宙ベース攻撃、OSC、CPP20081014563001、「軍事宇宙戦力の開発について」、中国軍事技術、2008 年 3 月

11 OSC、CPP20080123572009、「中国科学技術：軌道運動兵器の概念とその開発」、現代防衛技術、2005 年 4 月 1 日

12 Kevin Pollpeter、Leah Caprice、Robert Forte、Ed Francis 及び Alison Peet 共著、「超重要問題を抑制」、宇宙及びカウンタースペースに関連する中国軍事著作集、インテリジェンス調査分析センター、2009 年 4 月、32 頁

す核装置の爆発は、合衆国の核攻撃開始定義の赤線を突破するという著しいハイ・リスクに走らせることになる。さらに、EMP の標的行為は無差別であり、PLA は「錯綜した電磁環境」下で作戦を遂行させるため、部隊の訓練や準備を実施してはいるが、PLA 自身の宇宙ベース通信システムと、おそらくは地上の通信システムの大部分は、高高度又はより局地的な EMP 攻撃によって損害を被ることになる。少なくとも、EMP とその他の ASAT の類による攻撃は、PLA に対して、中国自身の急増する人工衛星群に対する報復攻撃をもたらすことになり、おそらくは中国の初期段階にある宇宙ベース C4ISR アーキテクチャーの機能を損なわせることになる。

中国の宇宙情報戦能力の完全な議論は、本調査が焦点としているコンピュータ・ネットワーク作戦(CNO)の範囲外である。とはいえ、この問題は、PLA の情報戦議論と中国軍組織における情報化分析の中核的存在となりつつある。

1.1　統合ネットワーク電子戦

現在の PLA IW 戦略に指針を与えている概念的枠組みは「統合ネットワーク電子戦(Integrated Network Electronic Warfare: INEW)」と題するものであり、敵の C4ISR ネットワークや他の主要情報システムに対して、コンピュータ・ネットワーク作戦(CNO)と電子戦(EW)を組み合わせ、連携して又は同時に攻撃するものである。この目的は、敵に戦闘作戦に不可欠な情報をアクセスさせないことである。

この戦略の採用は、PLA が戦時における、及びおそらくは平時も同様に、CNO の具体的役割を策定しつつあることを示唆している。

- ✧　また、PLA の軍事行動戦略は、CNO と EW を全作戦計画に統合するとした決意を反映したものとなっている。これによって、敵の情報センサーとネットワークを最初に攻撃し、情報優勢を獲得する。これは、他の部隊による戦闘行為に先立って行われるものと思われる。
- ✧　INEW 戦略は、EW による電子妨害、欺瞞、及び敵の情報の取得、処理と伝達能力の抑圧に依存している。CNA は、情報処理を妨害する意図で、「敵の知覚力を攻撃」することである[13]。

権威ある PLA 著者達は、INEW の様々な要素を首尾一貫して参照している。このことは、PLA の最高幹部による公式の審査を経たと明示する公開資料がないが、PLA が INEW を PLA の優勢 IW 戦略として採用したことを強く示唆するものである。

---

[13] OSC, CPP20020624000214、「統合ネットワーク戦及び電子戦について」、中国軍事科学、軍事科学院、2002 年冬

✧ INEW 戦略の考案者 Dai Qingmin 中将は、PLA の IW 能力近代化に係る多くの著書と率直な意見の持ち主である。彼は、早くも 1999 年の PLA 電子エンジニアリング・アカデミーの教授時代の「情報戦争入門」と題する論文や本において、電磁スペクトラム管理を抑制するためのネットワークと電子戦の組み合わせ利用について最初に記述した人物である[14]。

✧ 台湾のメディアは、Dai Qingmin 中将が PLA の 2002 年 PLA 内部報告において、PLA の統合ネットワークと電子戦を中核とした IW 戦略の採用を明らかにした、と主張している[15]。

✧ 2008 年 7 月、西安第 2 砲兵隊エンジニアリング大学の研究による PLA 情報セキュリティ・アーキテクチャ要求事項分析は、次のように言及している。「電子戦とコンピュータ・ネットワーク戦は、情報戦における 2 つの主要な攻撃モードである。・・・電子戦とコンピュータ・ネットワーク戦を組み合わせた利用、すなわち『統合ネットワークと電子戦』を利用することにより、敵の情報システムを完全に破壊するか、又はその機能を停滞させることができる」[16]。

✧ 2009 年の出典(脚注参照) [17]は、戦場における INEW 利用方法の簡潔な説明を次のように述べている。INEW は「電子妨害、電子欺瞞、隠蔽などの技術を利用した情報取得と情報伝達の中断、ウィルス攻撃又はハッキングによる情報処理と情報利用の妨害、及び新たなメカニズムによる対放射エネルギーやその他の兵器を利用した敵の情報プラットフォームと情報施設の破壊」を含むものである。

Dai は 2002 年、「統合ネットワーク電子戦入門」を出版した。これは、戦時における CNO 利用の戦略指針となる概念を公式に集大成したものである[18]。彼は同年、創意に富み影響のある論文において、統合されたネットワーク、センサー及び指揮組織に対する重要性の増大が、C4ISR システムの破壊と防護を中国の IW の中核にする、と論じた[19]。

✧ 両文書は、その草分け的な思考について賞賛を与えた統合参謀本部議長 Fu Quanyou 大将の強力な支持の下に出版された。彼の支持は、Dai1 の IW アプロー

---

[14] OSC, FTS20000105000705、「Fu Quanyou 推奨：IW に係る新陸軍本」、PLA 日報、1999 年 12 月 7 日

[15] OSC, CPP20071023318001、「台湾軍事書評：中国軍事ネット部隊、インターネット制御について」、Ch'uan-Ch'iu Fang-Wei Tsa-Chih、2007 年 3 月 1 日

[16] OSC, CPP20090528670007、「中国科学技術：PLA 情報システム・セキュリティ・アーキテクチャの構築」、コンピュータ・セキュリティ、2009 年 2 月 1 日

[17] OSC, CPP20090528670007、「中国科学技術：PLA 情報システム・セキュリティ・アーキテクチャの構築」、コンピュータ・セキュリティ、2009 年 2 月 1 日

[18] OSC, CPP20020226000078、「書評：統合ネットワーク電子戦入門」、北京、Jiefangjun Bao、2002 年 2 月 26 日

[19] OSC, CPP20020624000214、Dai Qingmin 著、「ネットワーク戦と電子戦の統合について」、中国軍事科学、軍事科学院、2002 年冬

チの強力な支援者となったこと、そしてついには彼を総参謀部第四部部長に昇進させたことを示唆するものであった。この第四部の担当は対電子対策の担当であるが、PLA の攻撃的 CNA 任務も担当すると思われる。

✧ Dai は 2000 年、総参謀部第四部部長に昇進した。同四部は、PLA の IW 任務及び PLA の情報戦に対する公式戦略としての INEW 両者に対する組織上の権限を整理統合したものと思われる[20]。

INEW 戦略の支持者は、敵が主要ノードを介してデータや兵站情報を指揮・統制していること、及びそれが戦略的目標となる軍事行動を支持することがほぼ断定できることから、INEW の目的が主要ノードだけの攻撃であることを明らかにしている。このことは、INEW 戦略が PLA の作戦計画立案者に影響を与えるものであり、IW の攻撃目標策定において、より質的な、かつ、おそらくは攻撃効果に基づくアプローチに向かうことが考えられる。

敵対者の情報システムに対する攻撃は、すべてのネットワーク、伝送及びセンサーの抑制を意味することでも又はその物理的破壊に影響を及ぼすものでもない。Dai やその他の者によるアプローチの要点は、INEW 戦略の意図する標的行為が、PLA の IW 作戦立案者が敵の意思決定、作戦及び士気に対してもっとも大きな影響を及ぼすと評価したノードに限定して実施されることを提案するものである。

✧ PLA の「軍事行動科学」は、IW における一つの役割が次であることに言及している。我が軍の IW 攻撃は、他の部隊が敵の「盲目」、「聾唖」又は「機能麻痺」の期間を利用して、敵に探知されることなく、又は敵の反撃リスクが低い状況で作戦遂行を可能とする機会の窓を開けるものである。

✧ Dai やその他の者は、INEW の適用によってもたらされた機会は、軍事攻撃の早期段階において優勢をもたらすことが確実なミサイル猛攻撃又は他の火力を用いた「ハード・アンド・ソフト攻撃」の組み合わせにより、速やかに利用されるべきであることを強調している[21]。

---

[20]IW 任務における総参謀部第四部のリーダーシップに関しては次を参照。James Mulvenon 著、「PLA のコンピュータ・ネットワーク作戦：シナリオ、ドクトリン、組織及び能力」、Beyond the Strait。Roy Kamphausen、David Lai、Andrew Scobell 共著、「台湾を除く PLA 任務」、Strategic Study Institute、2009 年 4 月、272～273 頁

[21] OSC, CPP20030728000209、「中国軍上級情報戦将校は統合ネットワーク/EW 作戦を強調」、北京、中国軍事科学、2003 年 4 月 20 日。OSC, CPP20020624000214、「中国軍上級情報戦将校が 4 つの能力要求事項を解説」、Jiefangujun Bao 著、2003 年 7 月 1 日。OSC, CPP2003728000210、「統合軍事行動における情報作戦のイデオロギー指針に係る PLA 定期刊行物」、2003 年 4 月 20 日。OSC, CPP2003728000210、Ke Zhansan 著、「統合軍事行動における情報作戦のイデオロギー指針の見本」、中国軍事科学、軍事科学院、2003 年 4 月 20 日。

✧ 2008 年 12 月付けの「中国軍事科学」AMS(軍事科学院。Academy of Military Science)定期刊行物に掲載された論文は、次のように断言している。PLA は、ネットワーク戦とその他の妨害を与える IW 要素の組み合わせを適用することにより、敵の意思決定能力に混乱又は損害を与えるとともに、敵の情報の流れを抑制し、情報優勢を獲得しなければならない[22]。

1.2 人民解放軍訓練における統合ネットワーク電子戦

INEW の構成要素を特徴付ける人民解放軍(PLA)の戦闘演習は、作戦計画立案者が軍事行動目的を支援するに当たり、この戦略を様々な部隊や訓練にわたってどのように統合しようと考えているのかを見抜く補足的な情報を提供している。CNA/CND/EW の組み合わせによる IW 訓練は、PLA のすべての部門及び軍区司令部から大隊又は中隊に及ぶすべての階層においてますます一般化されており、中国共産党総書記及び中央軍事委員会主席の胡錦濤の指導の下に、2009 年までに完全な情報化を達成するとした PLA の中核的能力と考えられている。

✧ 胡錦濤党総書記は、2006 年 6 月の全陸軍軍事訓練会議において、PLA に対し「複雑な電磁環境」を大々的に扱う訓練に焦点を当てよと命じた。この「複雑な電磁環境」とは、Jiefangjuan Bao の信頼できる論文によれば、複数階層の電子戦とネットワーク攻撃による作戦環境を意味する PLA の用語であるとされている[23]。

✧ 2004 年 6 月の間に行われた北京軍区の部隊による軍対抗演習において、仮想敵「青部隊」（PLA における敵部隊）は、演習開始後数分内に CNA を利用して赤部隊の指揮ネットワークに侵入・抑圧するとしている。これは、敵の C2 情報システムを戦闘の開始時に攻撃するとした INEW 戦略に従ったものである。PLA は、このような訓練を実施し、敵の戦術又は戦域指揮センター・ネットワークに対する標的行為の効果を評価しているものと思われる[24]。

✧ 2004 年 10 月、在来及び核ミサイル戦力を担当する PLA 第 2 砲兵隊の一旅団が訓練を実施した。その訓練は、大々的に INEW 要素を取り込むとともに、敵の EW 攻撃を防御しつつ、様々な支援部隊と司令部組織からなる多層階層通信を維持するネットワークで接続された C2 インフラに依存するものであった、と PLA は報告している[25]。

✧ 蘭州軍区の一師団が 2009 年 2 月に、敵のコンピュータ・ネットワーク攻撃と、その間の電子戦攻撃を阻止する防衛シナリオを大々的に取り入れた情報戦対抗演

---

[22] OSC, CPP20090127563002、Shi Zhihua 著、「情報作戦指令部の基礎的理解」、中国軍事科学、2008 年 1 月 27 日。
[23] OSC, CPP20060711715001、「JFJB 時事解説：情報化軍事訓練の促進について」、2006 年 7 月。
[24] OSC, CPP20040619000083、「ハイライト：中国 PLA の最近の軍事訓練活動」、2004 年 6 月 6 日。
[25] OSC, CPM20041126000042、「軍事報告：北京 CCTV-7 について」、2004 年 10 月 31 日。

習を行った。これは、ほとんどの情報化戦訓練に共通なものであると、PLA のテレビ・ニュース・プログラムは述べている[26]。

総参謀部軍事訓練及び兵器部の命令によれば、PLA の訓練ガイダンス「軍事訓練と評価の要点(Outline for Military Training and Evaluation: OMTE)」2007 改訂版は、全軍が PLA の中核となる軍事行動及び戦術訓練である複雑な電磁環境（Complex Elector-magnetic Environment: CEME)下での訓練を行うことを命じている[27]。**情報化環境における戦闘能力開発の焦点は、INEW 戦略の重要部分のほとんどを反映し、現在及び将来の訓練を洗練させ続けることであるとしている。このことは、Dai Qingmin の PLA 退役にもかかわらず、INEW 戦略が中国 IW の中核であり続けていることを示唆するものである。**

- ✧ PLA は、少なくとも 12 の情報化訓練施設からなるネットワークを構築した。これは、ジャミングや干渉が PLA 通信機能の低下を伴う現実的な多層戦闘訓練を大々的に取り入れた環境下で、部隊が交替で演習を実施できるようにしたものである。また、北京軍区の Zhurihe にある最新の施設は、「情報化青部隊」として常設された PLA の最初の部隊である。オープン・ソースの報告[28]によれば、これは北京軍区の第 38 陸軍集団第 6 機甲師団からの機甲連隊と思われる。この青部隊は、外国の戦術を採用するとともに、情報技術を広く利用した仮想敵対者である[29]。
- ✧ 闊歩 2009 という名称の PLA 大隊レベル部隊に対する大規模な多軍区演習は、これまでになかった 4 つの軍区からの部隊と PLA 空軍(PLA Air Force: PLAAF)の同時展開を大々的に取り入れたものである。この演習は、「2007 情報化訓練の訓練要点」に焦点を当てるとともに、複雑な電磁環境下での水陸両用車上陸、空爆、近接航空支援からなる複数任務シナリオを含めたものである[30]。

複雑な電磁環境下と情報化環境下の作戦に対する 2007 訓練指令の強調は、戦闘部隊の要員に対するスキル要求事項を満足させるため、攻撃的ネットワーク戦スキルを含む IW 専門家育成のための人的訓練の拡大をもたらす可能性がある。PLA は、専門家コース又はより上級学位授与プログラムの両者において、情報戦関連の教育を支援する大学及び研究

---

[26] OSC, CPM20090423017004、「Lanhou 軍区師団の情報対決演習の実施」、「軍事報告」ニュース放送から、CCTV-7、2009 年 2 月 2 日

[27] OSC, CPP20080801710005、「中国：JFJB 新軍事訓練、評価の要点の実施について」、2008 年 8 月 1 日。

[28] Asian Studies Detachment、 IIR 2 227 0141 09、「北京軍区第 6 機甲師団の情報システム近代化」、2009 年 1 月 29 日。

[29] OSC, CPF20081205554001、「北京軍区基地 EM 訓練向上が PLA 能力を促進」、2008 年 12 月 5 日。OSC, CPF20080912554001001、「PLA 青部隊が訓練の現実性を補強」、2008 年 11 月 12 日。Dennis J. Blasko 著、「今日の中国陸軍」、Routledge、2006 年、78 頁。

[30] OSC, CPP20090908088006、「闊歩 2009 演習における蘭州軍区師団が戦闘能力を増進」、Jiefangjun Bao 著、2009 年 11 月 12 日

所のネットワークを維持している。そのカリキュラムや研究の関心事は、PLA が強調するコンピュータ・ネットワーク作戦を反映したものとなっている。

- ✧ 上海の湖南区にある防衛技術国立大学(National University of Defense Technology: NUDT)は、中央軍事委員会の直接指揮下にある総合軍事大学である。NUDT には様々な情報セキュリティ教育コースがある他、同大学の情報システム管理学部とコンピュータ科学学部の教授陣は積極的に攻撃的ネットワーク作戦技術又は利用に係る研究を実施していると、NUDT 所属著作に係る引用検索からうかがわれる[31]。
- ✧ PLA 科学エンジニアリング大学は、先進の情報戦とネットワーキング訓練を提供するとともに、国防関連の科学、技術、及び軍事装備品の研究センターともなっている[32]。最近の IW 関連教授陣の研究の大部分は、ルートキット[33]の設計と検知に焦点を当てたものとなっている。これには、中国独自開発の Kylin オペレーティング・システム上におけるルートキット検知が含まれている。
- ✧ PLA 科学エンジニアリング大学は、PLA の職員に対し、様々な分野の先進技術学位を授けるとともに、情報セキュリティと情報戦を含む情報システムに係る全分野の訓練を実施している[34]。

1.3 戦争抑止とコンピュータ・ネットワーク作戦

中国政府は、どのようなタイプの CNA を一戦争行為として考えているのか明らかにしていない。このことは、危機における CNA の戦略的柔軟性を持ち続けるため、この件に関する情報を閉ざしたいとする願望の表れ以外の何ものでもない。中国の指導部は、台湾独立問題を除き、軍事力の行使基準として特定の「赤線」を引くことを一般的に避けている。これは、中国の CNA の適用にも通じることである。

- ✧ 効果的な戦争抑止には、必要な場合はそれを適用できる明確な決定の下に行動する有能で信頼できる軍事力、及びこの意図を潜在的敵対者に伝える手段が必要である、と軍事科学戦略は述べている[35]。
- ✧ また、軍事科学戦略は、抑止手段にはより大きな紛争を回避するための小規模な

---

31 NUDTの紹介については、次により入手可能である。
http://english.chinamil.com.cn/site2/special-reports/2007-06/26/content_858557.htm

32 OSC, FTS19990702000961、「中国は Jiang 法令により新軍事学校を設立」、新華社、1999 年 7 月 2 日。「中国は新軍事学校を設立」、人民日報、1999 年 3 月 7 日、次から入手可能。
http://english.peopledaily.com.cn/english/199907/03/enc_19990703001001_TopNews.html

33 クラッカーがコンピュータ・システムへの不正侵入後に利用するソフトウェア・パッケージをいう。

34 「中国は新軍事学校を設立」、人民日報、1999 年 3 月 7 日、次から入手可能。
http://english.peopledaily.com.cn/english/199907/03/enc_19990703001001_TopNews.html

35 軍事科学戦略、213～215 頁。

交戦が含まれることも強調している。CNA や EW などのツールは、多くの PLA IW 作戦において「無血」であると理解されている[36]。また、この概念は、中国の指導部が、情報ベース攻撃が敵対者の「赤線」を超えないと信じるならば、彼らは IW 兵器の先制利用をいとわない、という含みももっている。

また、PLA は、認知又は確信を具体化するための偽りの情報で敵の情報システムを侵すことにより敵の意思決定機能を攻撃目標とするため、IW を利用することも考えられる。「軍事科学戦略」は、これを IW が全軍事行動を支援できる主要な役割の一つであると強調している。データの改ざん又は破壊は、より広い戦略的心理作戦若しくは欺瞞作戦の支援ツール、又は抑止メッセージの一部としての認知管理目的支援ツールとして貴重なものであると理解されているようである。

- ✧ AMS 定期刊行雑誌が出版した広州軍区副司令官の 2003 年の論文「連帯軍事行動における情報攻撃と情報防衛」は、情報攻撃には敵の情報システム及び「認知と確信システム」の両者を攻撃目標とすることが求められると言及している。彼は、情報システムを攻撃する主な技法はネットワークと電子攻撃であり、人の認知と確信システムを攻撃する主な技法は情報欺瞞と心理的攻撃であり、これらは CNO によっても実施されると主張している[37]。
- ✧ IW 部隊の隊形に関する AMS ガイダンスは、部隊が敵に対する認知管理と欺瞞作戦を支援する心理的作戦要素を含めることを指令している。

CNO 支持者の中には、CNO が核兵器に匹敵する戦略的抑止能力であると認めている者もいる。かつ、CNO は核兵器に比べ、より高い精度を有し、負傷者はより一層少なく、そして PLA が保有するどの兵器よりも長距離の特性を有しているとしている。中国の信頼性のあるコンピュータ・ネットワーク攻撃能力の開発は、新核能力ミサイル、対衛星兵器及びレーザー兵器を含む、中国の戦略的抑止選択肢の拡大及び強化という大きな活動の一要素の位置付けにある。

- ✧ 軍事科学院の戦争理論・戦略研究所副所長 Li Deyi 中将は 2007 年に、情報抑止は戦略的レベルまで格上げされつつあり、核抑止に次ぐ唯一の重要性レベルを獲得するものであると言及した[38]。

---

[36]軍事科学戦略、213～215 頁。OSC, CPP20000517000168、「世界戦争、第三次世界戦争、完全な情報戦からの抜粋」、新華社、2000 年 1 月 1 日

[37] OSC, CPP20080314623007、「JSXS：連帯軍事行動における情報攻撃と情報防衛」、北京 Junshi Xueshu「軍事技術ジャーナル」、2003 年 10 月 1 日。

[38] OSC, CPP20081028682007、Li Deyi 著、「情報化戦争における思考モードの基本的特性に係る一考察」、中国軍事科学、2007 年夏、101～105 頁。

✧ 中国は、より精確かつ道路可搬の ICBM として米国本土を射程距離とする DF-31A、及び潜水艦発射用として最終的には中国の新 Jin クラス原子力潜水艦搭載の JL-2 を開発した[39]。

✧ 中国は 2007 年、運動撃墜手段を用いた直接上昇 ASAT 兵器のテストに成功し、中国の古くなった気象衛星を破壊した[40]。また、合衆国軍は 2006 年、一時的に偵察衛星を盲目状態にする中国のレーザー目くらまし兵器の利用について非難している[41]。

✧ 合衆国国防総省の分析結果によれば、中国の研究者は、合衆国の C4ISR 用の人工衛星やその他のコンポーネントに攻撃を行うことが可能な、様々な無線周波数兵器の開発に従事しているとしている[42]。

1.4 人民解放軍の情報戦計画立案

効果的な攻撃的 IW 能力には、所定のノード又は資産に対する CNA 攻撃の敵対者に及ぼす影響の程度について精確に評価する機能が必要となる。さらに、これらの評価は、敵対者のネットワーク、C2 関係、及びネットワーク上の具体的なノードに設置されている様々な付属物に係る詳細なインテリジェンスに依存する。

✧ 「軍事科学戦略」は、計画立案者に対して次を指令している。「作戦の重心を把握し、標的と攻撃順序を選定すること・・・・全運用システムと手順に及ぼす影響の程度に従い、作戦標的リストに対して選択的に敵の包括的弱点を配列すること」[43]

✧ また、任務計画立案者は、望ましくない付随的な損害又は防御上の重複を回避するため、定められたノードに係る明確な及び暗黙的なネットワーク依存性を理解しなければならない。防御上の重複は、標的の対象となった部隊又は組織がそのトラフィックを迂回させ、攻撃を「戦い抜き(fight through)」、中国の攻撃を効果的に無力化する可能性があるからである。

✧ CNA の計画立案に当たっては、所定の攻撃が敵対者にどのように認識されるかについて、その文化的又は軍事上の機微に対する微妙な理解が求められる。敵が利用する「赤線」[44]の理解を怠れば、意図しない紛争の拡大につながり、PLA に軍事行動目的の変更又は準備されていない完全に新たな軍事行動との奮闘を強いることになる。

---

39 議会年次報告「2006 年中華人民共和国の軍事力」、合衆国国防総省、3 頁。

40 議会年次報告「2009 年中華人民共和国の軍事力」、合衆国国防総省、14 頁。

41 Warren Ferster 及び Colin Clerk 共著、「NRO は中国のレーザー・テストが合衆国の宇宙飛行体を照射したことを確認」、宇宙ニュース・ビジネス報告、2006 年 10 月 3 日、次により入手可能：
http://www.space.com/spacenews/archive06/chinalaser_1002.html

42 議会年次報告「2006 年中華人民共和国の軍事力」、合衆国国防総省、34 頁。

43 「軍事科学戦略」、464 頁。

44 訳注：戦争開始への設定基準を超えることを意味する。

PLA の IW 計画立案者及び指揮官は、次のように言及している。CNO は、軍の作戦計画者がこれまで維持してきた「戦略」、「軍事行動」及び「戦闘」(西側の戦術に相当)の階層構成における区別を不鮮明なものにしている。したがって、戦術規模の部隊で採用された CNO と EW 兵器のほとんどは、在来兵器の射程距離を超え、敵対者地域の奥深くに位置する戦略標的を攻撃することができる。このことは、おそらく戦闘の推移を変えることになろう[45]。この IW、とりわけ CNO ツールに係る変化の見方は、上級指揮官の攻撃目標に対する見方に影響を及ぼすことになると思われる。

[45] OSC, CPP20081229563002、「戦略、軍事行動及び戦闘間の関係」、中国軍事科学、2008 年 12 月 29 日。

2　中国の紛争間におけるコンピュータ・ネットワーク作戦

CNO は、ミサイルや航空戦力の利用と同様に、紛争間において PLA 司令官が利用可能な戦闘能力をますます高めるコンポーネントの一つである。しかしながら、PLA は、CNO がスタンドアローン能力をもつものとして、他の戦闘分野から切り離して利用する議論をすることはほとんどない。西側の分析者や政策立案者が、中国の CNO に係る適切な前後関係の中で、大規模な軍事行動支援における CNO の利用方法を理解するには、中国の全軍事行動目的を考察する必要がある。ハイテク環境下における現在の軍事行動戦略は、ドクトリン的なガイダンス「敵のネットワークを破壊するには、敵のノードを攻撃せよ」[46]を反映したものである。このガイダンスは、指揮官に敵対者の C2 及び兵站ネットワークを最初に攻撃し、次いでその結果としての「盲目」状態を利用して、在来火力によるプラットフォームや人員攻撃を行うことを指示している。**この戦略は、PLA が紛争の開始フェーズにおいて CNO と EW 兵器を用いて攻撃し、敵の情報システムの機能を低下させることを示唆している。これは、従来の戦力対戦力による直接攻撃の企てでは、中国に比べ合衆国などの技術的先進国に対して不利となるからである。**

- ✧　戦闘作戦に不可欠な情報システムに対する敵のアクセスを断つ戦略は、従来の中国戦略の思考原則の影響を受けたものである。また、同戦略は、敵対者の弱点と重心についての広範囲にわたる現代の PLA 分析結果にもよると思われる。
- ✧　中国軍の指揮官は、ほぼ確実に中国の戦略的文化と伝承戦略の影響を受けている。中国現代軍事史のほとんどは、中国が明らかに弱い実体であった状況下における戦力投入意欲を反映している。この論題に係る学問は、短期間の紛争コストは戦略的条件が中国にとってあまり好ましくない後の情勢下におけるコストよりも低い、と常に判断した中国政党指導者を婉曲的に示している。この理論は、西側のくだけた評者にとってほとんど直観に反するように思えるが、変化する戦略的情勢の微妙なアセスメントの結果、及び好ましい結果を得るためのそれら情勢への最良の同調方法を反映したものである。PLA と中国の指導者は、弱者が強者に打ち勝つことを可能にする戦略、策略又は兵器を論ずる際、このアイデアを捕らえるのが一般的である[47]。

---

[46] 軍事科学戦略、464 頁。

[47]戦略的文化、戦争抑止、戦略及び中国の戦力利用傾向に係る現代学問分野はますます拡大しつつある。本調査研究の範囲を超えるものではあるが、現代コンピュータ・ネットワーク作戦に対するこれらのトピックの関係についての拡大論議は不可欠なものである。とりわけ、中国の権威ある書物の比較を超えた議論、及び現代中国の IW の理解と CNO の価値の複雑さを理解するという拡大された前後関係に向けての議論はなおさらである。中国の軍事力利用の入り組んだシステムに係る小規模な代表例は、次による。Allen S. Whitting 著、「中国の鴨緑江渡河：朝鮮戦争突入の決定」、スタンフォード大学新聞、1960 年。Allen S. Whitting 著、「1960 年～1996 年における中国の軍事力利用、及び台湾」、情報セキュリティ、第 26 巻、No.2、2001 年秋、103～131 頁。Alastair Iain Johnston 著、「軍国主義が吹き込まれた中国の国際論争態度 1949 年～1992 年：編集済み本編」、中国定期刊行物、1998 年、No.153、1998 年 3 月、1

✧ PLA の CNO の利用は、統合－そしてますます連帯を高めた―軍事行動能力の一エレメントとして（EW 兵器と合わせて）CNO を利用する意図を反映したものである。軍事行動ドクトリンは、情報優勢獲得の先達として CNO を利用し、これにより「開口部」、すなわち陸海空軍部隊による作戦遂行の機会を与えることを求めている。

中国の CNO は、中米間軍事危機の全ての場面において、国防総省の兵站と指揮統制機能を支援する NIPRNET ノードに対し、持続的な攻撃を行うために利用されると思われる。このような攻撃は、合衆国の情報と支援システムに十分な機能低下を起こさせることを意図しており、これにより PLA は、合衆国とその同盟国が十分な軍事力で PLA の作戦遂行を頓挫又は退化させる対応行動に移行できる前に、PLA の軍事行動目的を達成するのである。PLA の計画立案者は、台湾に係るシナリオの場合、CNO 利用による作戦遂行機会を台湾島での軍事目的を達成するには不可欠な機会の窓として検討していると思われる。合衆国の軍事対応を遅延させる CNO やその他の IW 兵器は、優勢な合衆国軍隊との直接戦闘を必要とすることなく PLA の成功確率を高める以外にない。

✧ 台湾シナリオにおける合衆国の戦闘作戦の遅延又は能力低下は、PLA の台湾占領又は同島の政治的リーダーシップの降伏強制の達成を許すものであり、合衆国が戦闘作戦地域に到着した際の「既成事実」となっている。
✧ 合衆国軍事兵站情報システムのほとんどは NIPRNET を介して伝達又はアクセスされ、これにより軍のグローバル・サプライ・チェーンにおける数百にも及ぶ民間と軍のノード間の通信又は調整を促進している。

2.1 兵站ネットワークとデータベース

戦闘間における NIPRNET ベースの兵站ネットワークは、中国の CNA と CNE の高優先順位標的になると思われる。主要兵站ハブにおける情報システムは、それが合衆国太平洋軍(US Pacific Command: USPACOM)作戦地域(Area of Operation: AOR)又は USPACOM 作戦を支援する米本土地域にあろうとも、紛争間においては中国の CNA と CNE 作戦の対象になると思われる。中国は、合衆国軍の尻尾のように長い兵站と長期に及ぶ部隊終結時間を、利用すべき戦略的ぜい弱性及び重心として把握している。

✧ イラクにおける合衆国軍事行動（砂漠の嵐とイラク自由作戦の両者）、バルカン諸

～30 頁。Alastair Iain Johnston 著、「文化的現実主義：中国歴史における戦略的文化と総括的戦略」、プリンストン大学新聞、1998 年。M. Taylor Fravel 著、「不安定な政権と国際協力：中国の領土論争における妥協について解説」、国際安全保障、第 30 巻、第 2 号、2005 年秋、46～83 頁。Thomas J. Christensen 著、「風と戦争：傾向分析と北京の軍事力利用」、中国の対外政策研究における新たな方向、Alastair Iain Johnston 及び Robert Ross 共著、スタンフォード大学新聞、2006 年。

国及びアフガニスタンに対する PLA のアセスメントは、兵站と部隊展開時間が弱点であり、それらに対する妨害が軍需物資の供給遅延又は欠乏をもたらすことを明らかにしている。これらのアセスメントは、概して、兵站システムを頓挫させることが事実上合衆国軍の頓挫につながるのではなく、兵站システムに対し混乱を及ぼすことが PLA にとっては上述のように「時間かせぎ」になる、と示唆しているように思える。

- ✧ PLA の計画立案者が関心を抱いている兵站データは、具体的な部隊展開スケジュール、資材の再供給と移動計画、部隊態勢完了アセスメント、積載能力と時間表作成、海上事前展開配備計画、地域給油作戦に対する航空任務命令、西太平洋戦域所在基地の兵站状況などである。
- ✧ 合衆国統合参謀本部出版物「USJP-4：統合兵站」は、「統合軍のグローバルな展開と脅威発生の急速性は、軍事作戦の支援に当たって、情報のリアルタイム又は近リアルタイムを不可欠なものとしている。効果的な意思決定を行うには、継続したアクセスを伴う統合兵站計画の立案、実施、管理が必要である。ネットワークに対する保護されたアクセスは、統合軍の準備態勢完了と統合戦力軍(Joint Force Command: JFC)の要求事項を満足させる迅速で厳格な対応を可能とするために不可欠なものである[48]。
- ✧ 合衆国輸送軍(US Transportation Command: USTRAMSCOM)ネットワーク・トポロジー又は NIPRNET に接続された USTRAMSCOM 関連兵站部隊に関する中国側の熟知能力は、具体的な緊急事態又は作戦計画に対して段階的に計画された部隊展開データ(time-phased force and deployment data: TPFDD)に関連するデータにアクセスし、それを盗み出すとした中国の CNE 任務を助けることができる。TPFDD は、補給物品の移動順序に対する兵站の「ブループリント(詳細な計画)」であり、司令官の戦闘戦域に対する人員及び資材移動の優先順位を示すものである。

中国は、軍の重要な補給物品と人員の移動支援を行う戦略的な民間港湾施設、出荷ターミナル又は鉄道に関連した潜在的にぜい弱なネットワークに対して、標的行為を企てると思われる。主要な流通間における移動管理を効果的に維持することは、本質的に複雑なものである。主要ノードの情報システムの混乱、とりわけ壊滅的な状況下に陥っていない場合の出荷ターミナル又は空港の「下流部門(downstream)」における混乱は、ラッシュ時の小規模偶発事故に起因する輸送遅延の連鎖と同様に、影響を被った出荷先への輸送途中での遅延又は輸送停止が強いられることから、大きな遅延をもたらすことができる。

- ✧ 合衆国統合参謀本部出版物「USJP-4：統合兵站」は、「信頼性のある情報（正確、

[48]「USJP-4：統合兵站」、2008 年 7 月 18 日、合衆国国防総省、1～5 頁。次により入手可能：http://www.dtic.mil/doctrine/jel/new_pubs/jp4_0.pdf

実時間かつ高い可視性のある情報）と成果に基づく在庫管理は、サプライ・チェーン中の資材インベントリ属性に係る意思決定の基調をなす傾向にある。最善の保管レベルと資材に対する説明責任をサプライ・チェーン中に維持することは、統合兵站による戦略及び戦術サプライ・ノード間の資材の流れの管理を可能にし、戦闘員の要求事項を満足させることになる」[49]とも指摘している。

- ✧ NIPRNET 上にある多くの兵站データベースは、ウェブ・ベースのインタフェースによりアクセスが容易なものとなっている。したがって、PLA のオペレータは、単に、キーストローク・ロギングを介して弱いパスワードを入手するか、又はウェブサイト上に SQL インジェクションぜい弱性を利用して、ユーザーもどきのアクセス権を入手するだけとなる。
- ✧ PLA は、CNE 技法による長期間の NIPRNET へのアクセス、とりわけ様々な戦闘計画に対する TPFDD 支援兵站情報へのアクセスによっても、特定の不測事態を意図した合衆国軍展開パッケージに対する詳細な最新インテリジェンス様相を組み立てることができる。

PLA の NIPRNET 兵站データベースに対する基本的 CNE/CNA 戦略は、選定したネットワーク・セグメント上の暗号化されていないデータ・フローの制限、そしておそらくはデータの改ざん両者の組み合わせ攻撃によるものと思われる。兵站情報システムに対する攻撃は、一種の危機発生時の決戦時に出動する戦争予備軍として、予め危殆化されたネットワーク上のホストを利用して開始されるものと思われる[50]。

- ✧ PLA オペレータは、仮に、HTTP トラフィック（一般的なインターネット･トラフィック）がネットワークから伝送される前にプロキシ・サーバーを介して認可されてなければ、このような部隊又はネットワーク･セグメントを標的にすることで、ネットワーク上でより自由に活動することができる。このような環境下における攻撃者は、リモートの C2 ノードに接続することにより、ユーザー証明書の確認を求められることなく追加のツールをダウンロード又はデータの密かな窃盗や潜入行為を行うことができる。

中国が関与した合衆国ネットワーク攻撃に係る報告は、これらのオペレータが職務又はアクセス情報からの推定により、部隊又は組織の特定ユーザーを識別することができる能力をもっていることを示唆している。正当なユーザー証明書を利用した攻撃者のアクセスは、任務要求事項と合衆国インフォコン(INFOCON：情報作戦準備態勢)レベルにもよる

---

49 「USJP-4：統合兵站」、JP-40 頁。

50 攻撃技法は、合衆国の INFOCON レベルの変化に応じてシフトすると思われる。INFOCON は、アプリケーションへのアクセスを制限するか、又はネットワーク上のトラフィックに関して外部接続と優先順位を制限して、ファイアウォールを介してインバウンドが許可されるトラフィックに影響を及ぼす。

が、ファイルのディレクトリを見ることや窃盗や改ざんの対象となる特定ファイルへの標的行為を許す可能性がある。そしてこれらのオペレータは、このアクセスを利用することにより、インテリジェンス収集目的でネットワーク・トラフィックの受動モニタリングを行うことができる。攻撃者は、平時においてこれらのマシンにツールをインストールすることで、危機発生時に利用可能な戦争予備軍として予め危殆化することができる

- ✧ 中国の CNO オペレータは、ルートキットと密かなリモート・アクセス・ソフトウェアの作成、及びこれらのアップロードを行うための高度の技術を持っているようである。そしてオペレータは、この技術を駆使して危殆化されたホストへの執拗なアクセスを継続するとともに、防御側の検知を極めて困難なものにしている。
- ✧ また、作戦部隊の兵站支援を行っている民間契約者ネットワークに対する「上流(upstream)」攻撃も、大きな影響をもたらす可能性がある。そして、洗練されたネットワーク・セキュリティとモニタリングに対する資源又は専門知識がたいてい欠落している小規模会社に対しては、より容易に攻撃が行われる可能性がある。
- ✧ 上記に述べたぜい弱性に係る要点の多くは、ネットワークにプロキシ・サーバーの設置、プロキシ・サーバーを経ないアクセスをブロックするファイウォールの設定、ユーザー認可確証なしのプロキシへのアクセスのブロック、及びユーザーの保証書を攻撃者から保護することにより、大幅に最小限化することができる。

また、中国の CNO オペレータは、誤った記録のアップロード又は既存の記録を改ざんすることにより、合衆国がこれらのネットワーク中のデータの正当性を確認することを意図した攻撃を企てると思われる。このような攻撃を発見するには、部隊が通常運用を開始する前に、マンパワーと資源を集中的に割り当て、標的となった部隊のデータベース記録やその他のファイルと、正しいバックアップ・コピーとを比較したレビューが必要となるが、犠牲の多い運用遅延になる可能性がある。仮に、この種の攻撃がいくつかの大きな又は重要なサプライ・ノードに対して展開されれば、その影響は重大なものとなる。

- ✧ PLA オペレータが、NIPRNET の兵站データベース上にファイルをアップロードすることや既存のレコードをアクセスするためには、標的とした LAN 上のコンピュータの危殆化とローカル・ユーザーの証明書が必要である。過去において、中国が関与したと考えられた合衆国ネットワーク侵入に対する観察結果からは、PLA オペレータにこの能力があると判断されている。
- ✧ この種攻撃の発見は、より局地的な標的行為による供給あて先変更に比べ、認知管理又は心理作戦の観点から合衆国部隊に大きな影響を及ぼすものである。
- ✧ 情報セキュリティ上の懸念から、全戦域又は米本土のシステム管理者や兵站要員が時間を費やすこととなる兵站又は他のデータベースの確認が必要となる場合、合

衆国の作戦遂行上の速さに不相応な影響をもたらす危殆化はほんのわずかで十分である。

2.2　指揮・統制データ

部隊の位置、状況、状況報告、展開命令など、司令部組織と隷下部隊間における作戦遂行上のトラフィックの大部分は、平時及び戦時とも秘密区分指定システムを介して伝達される。CNO が、これらのシステムのアーキテクチャーに構築された暗号と防衛階層に侵入の上、危殆化する場合、中国の IW 部隊又はそれらを支援すると思われる民間人研究者には資源集中型及び時間消費型プロセスが必要となる。**敵の情報の流れを攻撃するに当たっての中国のドクトリン上の方針は、次を示唆している。仮に、秘密区分指定ネットワークが攻撃されるとすれば、その意図はデータの解読や活動中のネットワークに侵入することではなく、非秘密区分指定バックボーン・ネットワーク中に流れている暗号化されたデータの伝送を遅延させることであると思われる。**

- ✧　たとえ、機微な暗号化されたネットワークが危殆化を免れたとしても、コンピュータ・ネットワーク・エクスプロイテーション(CME)による暗号化通信に焦点を当てたトラフィック分析は、今なお有用な情報を提供する。
- ✧　仮に、PLA CNO オペレータが特定の合衆国軍部隊のネットワーク又はデータベースに対する標的行為任務を付与された場合、平時における基本的なネットワーク偵察の実施は、戦時における攻撃作戦を支援することができる。
- ✧　攻撃者は、これらの部隊又はデータベースがいったん識別されれば、一般的な技法又はツールを利用し、全てのサーバー又はルーターに対してサービス妨害攻撃による影響を及ぼすことができる。この攻撃の精巧さは、中国ハッカー・コミュニティ内の多くの個人に対して評価した技術能力の範囲内であり、訓練された CNO オペレータからなる PLA 部隊の精巧さも同様と思われる。
- ✧　CNE 作戦のあるものは、純粋に偵察目的に向けられたものであり、ネットワーク・トポロジーを精密に記すとともに、特定地域における合衆国軍又は商用ネットワークに係る指揮・統制関係を把握することであって、データを密かに盗み出したり又は「眠っている(sleeper)」マリシャス・ソフトウェアを攻撃目標のマシンに埋め込んだりするものではない。

PLA CNO の指揮官とオペレータは、平時における危殆化能力が戦時におけるアクセスを保証するものでないことを認識していると思われる。US INFOCON のレベルは戦時において格上げされ、敵対者が何らかの操作を行ったマシンの一部又は全てに対するアクセスが阻止される。しかしながら、現在行われているプロービング(コンピュータ・ネットワークの状態を探ること)や危殆化は合衆国の防衛態勢の変化を誘い出すものであり、脅威が

高まったネットワーク環境下における変更がどうなるのかについて、何らかの識見を与えることになる。したがって、中国の作戦には、合衆国の対応を誘い出す意図的な「雑音(noise)」を発生する活動が含まれており、これによって、攻撃者は合衆国防衛態勢が特定の環境下においてどのように変化するかについてのインテリジェンスを収集することができる。これはサイバースペースに関連するものであり、合衆国が冷戦時代に電子戦作戦の一環として様々な脅威に対するソ連の対応に係るインテリジェンス収集を目的として行ったソ連防空ネットワークへの挑発行為に類似している。

3　中国のコンピュータ・ネットワーク作戦における主要組織

3.1　総参謀部第 4 部

これまでの総参謀部(General Staff Department: GSD)第 4 部の攻撃的 EW 任務、同部に対する最近 5 年間の Dai Qingmin のリーダーシップ、及び INEW 実施における同部の役割に触れているオープン・ソース報告のすべては、同部が PLA における攻撃的 IW の主たる権限をもっていることを示唆している。

- ✧　また、第 4 部は、対電子対策(Electronic Countermeasures Department: ECM)部とも言われており、ECM 作戦部隊と様々な攻撃的 IW 技術の研究を実施している研究開発機関の両者に対する監督も実施している。
- ✧　第 4 部による IW 監督の実施は、少なくとも 1999 年にさかのぼるが、おそらくはそれ以前から実施されていたと思われる。最近の研究成果は、Dai Qingmin の創意に富んだ影響力の大きい研究「情報戦について」が、その 1999 年の出版に先立ち第 4 部の審査を受けたことを言及している。このことは、その当時でさえも、組織的な監督を受けたことを示すものである[51]。
- ✧　2000 年に Dai Qingmin を第 4 部長に昇進させた GSD の決定は、彼の INEW 戦略に係る提唱を審査の上、おそらくは IW と CNA 任務に係る組織権限を特にこの部に整理統合したことによるものと思われる。Dai の部長昇進は、INEW を PLA の IW 戦略として適用するとした彼の先見性について、おそらくは GSD が支持したことを示唆するものである。

3.2　総参謀部第 3 部

GSD 第 3 部は、シグナル・インテリジェンス(SIGINT)が長年の間活動の中心なっていること、歴史的に見ても攻撃的役割が欠落していること、及び外国語と技術的スキルが堪能な大勢のスタッフが在籍していることから、PLA における CND と CNE 任務に対する監督に十分適したものとなっている。同部は、PLA の各軍区本部に収集処理機能を備えたシグナル収集所を設置し、中国全土に及ぶ広大なシステムを維持している。同部の任務は、外国のシグナルの収集、利用及び分析である[52]。また、PLA の音声及びデータ・ネットワークの通信秘匿任務も付与されている。この後者の責任事項は、ネットワーク防衛についても含まれると思われる。もっとも、この役割を確証付ける情報はあまりない[53]。西側の

---

[51] Mulvenon著、「PLAコンピュータ・ネットワーク作戦」、272頁。OSC, FTS20000105000705、「Fu Quanyou推奨：IWに係る新陸軍教本」、Jiefangjun Bao著、1999年12月7日。

[52] Desmond Ball 著、「中国におけるシグナル・インテリジェンス」、Jane's Intelligence Review、1995 年 8 月 1 日。

[53] OSC, CPP20060110510011、「HK ジャーナル: 中国インテリジェンス局の詳細な歴史、構成、機能」、香港 Chien Shao、No 179、2006 年 1 月 1 日。Mark A. Stokes 著、「中国の戦略近代化：合衆国に及ぼす影響」、合衆国陸軍研究所、1999 年 9 月、34 頁。

同部に係る分析には、130,000 名以上のスタッフが在籍していると主張するものもあるが、この数値の正しさを確証するものはない。このような具体的なスタッフ人数はさておき、大勢のスキルの高い語学堪能者及び技術分析者が在籍しているということは、コンピュータ・ベースのインテリジェンス収集及び利用任務遂行に当たって、第 3 部が高度の知識を提供していることを示すものである。

図 1 は、人民解放軍(PLA)総参謀部の組織図を示すものである。

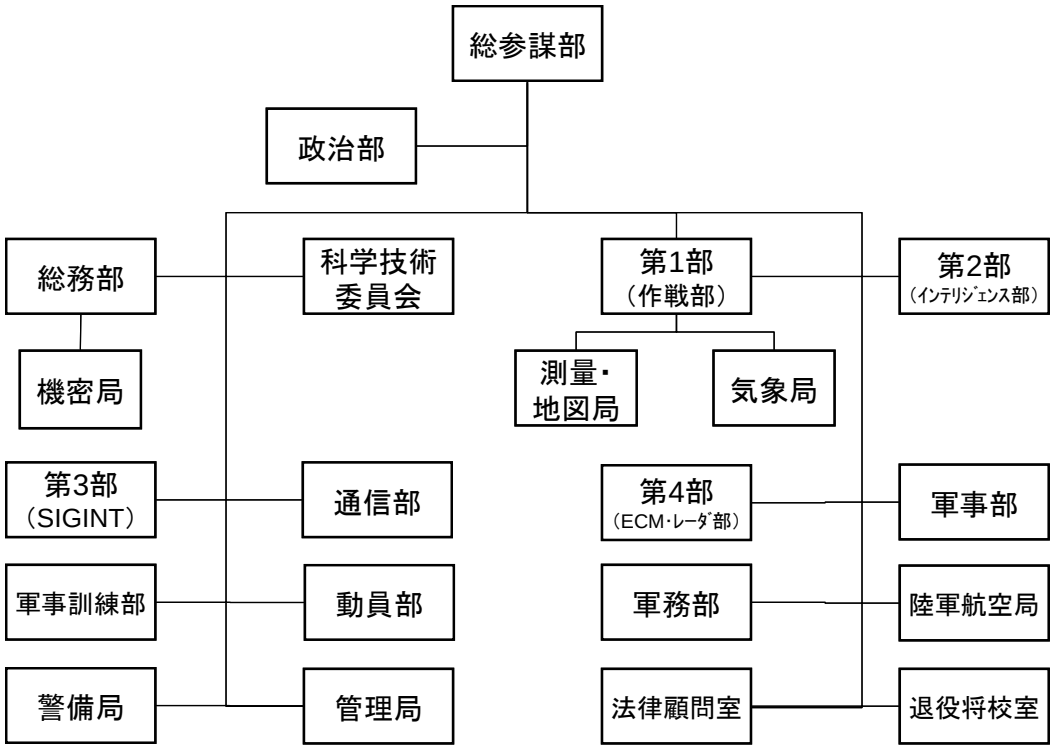


図 1：人民解放軍総参謀部[54]

3.3　技術偵察局

PLA は、少なくとも 6 つの技術偵察局(Technical Reconnaissance Bureau: TRB)を維持している。これらは、蘭州、済南、成都、広州及び北京の各軍区にあり、戦術及び戦略目標に対する SHIGINT 収集任務に加え、CNO 任務ももっている。もっとも、これら部隊の確かな役割や従属関係についての情報はほとんどない[55]。TRB は第 3 部との従属関係に

[54] 組織図の出典：James C. Mulvenon 及び Andrew N. D. Young 共著「人民解放軍組織参照 Vol1.0」における David Finkelstein 著「中国人民解放軍総参謀部：組織、役割及び任務」、RAND 社、2002 年

[55] Roy Kamphausen及びAndrew Scobell共著「人民解放軍規模の適正化：中国軍の概略を調査」におけるDennis Blasko著の「PLAの陸軍近代化と任務の多様化：全軍区において実施中」、戦略研究所、2007年9月、366～372頁。Ellis L. Melvin著、「中国人民解放軍陸軍区本部技術偵察局の調査」、2005年6月19日。

あると思われる。このことは、彼らの CNO 任務が外国のネットワーク防衛とエクスプロイテーションに焦点が当てられていることを示唆するものである。TRB の活動の中心は従来からの SHIGINT 任務がほとんどであると思われる。しかしながら、これらの部隊が情報セキュリティ又はことによると関連する論題の先進的研究を行っているとする間接的な言及からは、彼らが SHIGINT 収集任務を拡大した CNO 又は EW の役割を担っていることが示唆される[56]。

- ✧ 党関連の新聞報道は、TRB 所属スタッフが他の PLA 部隊に対する情報保証検定業務も実施していると伝えている[57]。
- ✧ 地方共産党関連報道局は、第 3 部が 2002 年に「技術即応部隊」であると評され、優れた「情報戦理論研究」成果及び新技術的作戦遂行手段の開発に対し、連続 5 回目の栄誉を得たと伝えている。これらの日付と番号は、早くも RTB が 1997 年に、その任務に IW を含め始めたことを示唆するものである[58]。
- ✧ PLA 報告は、成都軍区の第一 TRB が「情報化構築における多大なる業績」、アカデミック研究賞、及び GSD レベルの技術評価による利用審査を経たコンピュータ・ネットワーク防衛に対して一連の軍事的賞賛を得たと伝えている[59]。

3.4 人民解放軍情報戦民兵部隊

人民解放軍(PLA)は約 2002 年以来、IW 民兵部隊を創設してきた[60]。この部隊は、民間 IT セクター及び大学の要員から構成され、PLA CNO 作戦と中国市民情報セキュリティ専門家間の運用上の結びつきを代表するものである[61]。PLA は、全中国の民間会社内にじか

「仮想情報センター、人民解放軍入門書」、2006年8月4日、次により入手可能：http://www1.apaninfo.net/Portals/45/VIC_Products/2006/08/060804-P-China.doc.

56 OSC, CPP20071011318004、「成都軍区78006部隊、最先端IT研究における飛躍的前進を賞賛」、成都 Zhangi Bao、2007年8月20日。OSC,CPP20070122478002、「瀋陽軍区65016部隊員、情報戦は情報化戦ではない」、2007年1月22日。

57 OSC, CPP20081211478016、「PLA65016 部隊、ネットワーク・セキュリティ・チームが包括的セキュリティ検定を実施」、成都 Zhangi Bao、2008 年 10 月 18 日、1 頁。

58 OSC, CPP20030411000212、「中国 C4I 活動総括：2002 年 11 月 5 日～2003 年 3 月 12 日」、2002 年 11 月 5 日。Ellis L. Melvin、同書。

59 OSC, CPP20081113563001、「中国：PLA 活動報告、2008 年 10 月 1 日-15 日」、2008 年 11 月 13 日。

60 PLAの800万人規模の民兵システム、これは国務院と中央軍事委員会(Central Military Commission: CMC)の管理下にあるが、18歳～35歳の男子から構成される予備軍システムであり、PLA軍務に就いているわけではない。民兵システムは、事実上、全ての軍事作戦におけるPLA部隊の活動任務を増強するものである。「2004年中国の国防」、中国国務院情報室、2004年12月、http://english.peopledaily.com.cn/whitepaper/defense2004/defense2004.html を参照。「2006中国の国防」、中国国務院情報室、2006年12月、北京、次により入手可、http://english.chinamil.com.cn/site2/newschannels/2006-12/29/content_691844.htm。

61 OSC, CPP20031002000138、「民兵情報戦エレメントとして広州における電気通信専門家を倍加する」、Guofang、軍事科学院、2003 年 9 月 15 日。OSC、「PLA C4ISR 活動総括」、2006 年 4 月～5 月 30

に民兵部隊を設立した。これは、先進教育を受け、現代の商業用基盤で洗練されたソフトウェア設計能力を持ち、かつ、「政治的に信頼できる」技術者に直接アクセスできる利点があるからである[62]。

- ✧ 広州人民武装警察(People's Armed Police: PAP)守備隊の一政治委員は 2003 年、情報戦、電子戦及び心理戦における都市圏の民兵部隊に対する直接関与を提唱した。彼は、民兵部隊の改革努力の焦点を、広州民兵の主要任務の一つとして、情報戦を加えることに当てるべきであるとも提言した[63]。
- ✧ 天津に配置されている民兵守備隊が 2004 年、情報化環境における作戦遂行能力を増強するため、専用の情報作戦部隊の創設を含め隷下部隊の改革を行った、と PLA 日報が伝えている[64]。
- ✧ 河南省小軍区は 2007 年、通信及びネットワーク戦争民兵組織を創設した。そして安徽省の部隊は 2008 年から、特殊技術訓練の教官要員として大企業の民兵隊員をリクルートし始めた、と PLA メディアが伝えている[65]。

PLA 報道は、IW 民兵部隊が攻撃的と防衛的な CNO と EW、心理戦及び欺瞞作戦の任務を付与されたことを明らかにした。もっとも、入手可能な情報源からは、それらの権限範囲、従属関係や任務の具体的内容は不明である[66]。

- ✧ 永年県の民兵大隊(寧夏省、蘭州軍区)は 2008 年 3 月、IW 民兵グループを確立し、ネットワーク戦研究と訓練及び「戦時における敵のネットワーク攻撃」の任務を付与した、と同部隊のウェブサイトが伝えている[67]。
- ✧ 永年部隊は、情報戦センター派遣隊、情報収集派遣隊、民兵ネットワーク戦部隊及び民兵ネットワーク防護部隊から構成されている[68]。これは、この部隊が CNO

日。

62 OSC, CPP20031002000138、同書

63 Lu Qiang 著、「民兵構築を強化するための情報戦の特性に焦点を当てて」、中国民兵雑誌、2003 年 8 月、次により入手可能、http://www.chinamil.com.cn/item/zgmb/200308/txt/16.htm。

64 OSC, CPP20050301000186、「中国における C4I 活動報告:2004 年 11 月 13 日～2005 年 1 月 15 日」、2005 年 1 月 15 日。

65 OSC, CPP20080601711001、「目次報告:中国民兵(Zhongguo Minbing)」、2008 年 3 月 10 日。OSC, CPP20080615711001、「目次報告:中国民兵」、2008 年 4 月 10 日。

66 「ネットワーク戦民兵部隊の任務」2008年3月16日、次により入手可:
http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp?infoNo=26366。中国と北アジア、「ジェーンのセキュリティ・アセスメント・センティネル」2009年4月3日。OSC CPP20090102670001、「中国科学技術:Ezhou 民兵がネットワーク駐留を確立」、Guofang、軍事科学院、2001 年 5 月。OSC, CPP20031002000138、「広州電気通信専門家を民兵情報戦分隊として倍加」、Guofang、軍事科学院、2003 年 9 月 1 5 日。

67 「永年が最初の情報戦民兵部隊を設置」、2008 年 3 月 19 日、次により入手可:
http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp

68 「ネットワーク戦民兵部隊の任務」、2008 年 3 月 16 日、次により入手可:

任務に係る全分野に対して責任をもっていることを示唆するものである。

図 2：蘭州軍区永年地区情報作戦民兵部隊室、

図 3：永年郡情報戦民兵成立大会

軍事科学院(Academy of Military Science: AMS)は 2003 年当初、広州軍区における IW 民兵部隊設立構想開始の確かな証拠となる報告書を出版した。これは、地方に所在する電気通信会社を基盤として利用し、そこから要員、財政的支援及びインフラ・アクセスを引

http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp?infoNo=26366

き出そうとするものである。このことは、PLA が軍の情報戦要求事項を支援するものとして、ますます成長し続けている民間企業の IT 専門家予備要員団のエネルギーを取り出すものと示唆される。広州守備隊は、CNO と攻撃的及び防衛的 EW 部隊から構成される 4 つの「民兵情報技術大隊」を地元の会社に創設した[69]。

- ✧ 将校は、IT セクターが集中している広東東山地区の詳細な調査を実施した。これは、先端技術学位の保持者、海外留学経験者、主要な科学研究成果を成し遂げた人物、コンピュータ・ネットワーク専門家など、特殊な経歴をもつ要員を明らかにするものであった。このことは、この部隊の任務が、先進技術専門知識及び外国語又は文化知識の両者をもつ要員を必要とする、より洗練されたネットワーク作戦であることを示唆するものである[70]。
- ✧ この大隊には、本部部隊、攻撃小隊と防衛小隊からなる CNO 中隊、及び電子偵察小隊と欺瞞小隊からなる EW 中隊が含まれる。
- ✧ この部隊創設の責任将校によれば、これに先立つ部隊レベルの訓練資料は存在していないとしており、このことが、広州軍区本部部隊及び明示されていない「電子対策連隊」、これは GSD 第 4 部の隷下部隊と思われるが、からの入力に基づき「民兵情報技術分隊訓練計画」の草稿作成を強いることとなった。訓練資料が欠落していることは、このような部隊の創設はごく最近であり、おそらくは AMS による審査中である証拠を示唆するものとされる。

この大隊の研究任務には「ハッカー攻撃、ウィルス繁殖、情報チャネル妨害及び敵ネットワーク・ノードの混乱」に対する作戦手法が含まれる。このことは、特別な部隊が存在し、CNE 作戦遂行任務に加え、攻撃手法の研究開発任務が付与されていることを示唆するものである[71]。

AMS は広州の部隊創設後 3 年以内に、IW 民兵編成の推奨を明示した構想に係る第二の論文を出版するとともに、PLA に対しこれら部隊の優先的創設を指示した[72]。そして提示されたモデルは、これより 3 年前に広州守備隊が創設した部隊を模範とするものであった。このことは、IW 民兵組織の編成が今や完全に精査された上級指導者の命令であることを示唆するものである。

---

69 「ネットワーク戦民兵部隊の任務」、2008 年 3 月 16 日、次により入手可：
http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp?infoNo=26366。

70 OSC, CPP20031002000138、2003 年後期に出版されたこの論文には、この部隊創設の正確な日付が明示されていない。しかしながら、我々が実施したこれら部隊の一連の技術業績の関連付け結果からは、この大隊が論文記述時に運用開始となったことが示唆される。

71 OSC, CPP20031002000138。

72 OSC、「PLA の C4ISR 活動総括」、2006 年 4 月 1 日から 5 月 30 日。

- ✧ AMS は、守備隊レベルの司令部に対し、地元の民間 IT 企業や大学の要員によりこれらの部隊を創設するとともに、彼らのスキルを IW のあらゆる面において向上させるため、ネットワーク環境をシミュレートした訓練を実施することを命じた。この訓練は、電子戦、ネットワーク戦及び心理戦の遂行に当たって、スキルを備えた特殊部隊を創設するためのものである[73]。
- ✧ また、守備隊の司令官は、民兵の標準年齢と身体的適合要求事項を緩和することについても指示された。これは、高価値の技術スキルをもつ人物を不必要に排除しないためと思われる。

これら部隊に対する典拠が確かな PLA 出版物は、これらの部隊が外国のネットワークを標的にしているとさらけ出されることによる外交に及ぼす影響の可能性、又は部隊のツールが部隊の管理外に置かれる可能性があることについて、細心の注意を怠らないことを明確に表明している。AMS はこれを受けて、民兵部隊に対し通常とは異なる厳格なセキュリティ予防処置を、とりわけ要員の審査と監視において講ずるよう勧告したと思われる。これは、これら部隊の極めて機微な業務を反映したものと判断される。

- ✧ AMS の 2006 年の出版物は、多くの国々がネットワーク偵察、電子妨害及び「ネットワーク侵入」を重要課題としており、戦争に関する法令さえも考慮していると言及している。PLA の明確な認識が表面に出ることはめったにないが、これはその一つである。
- ✧ 守備隊の司令官は、「個人の振る舞いは監視され、作業結果が外部に漏れることはない」ことを確実にするよう追い立てられている。可能性のある AMS の言及としては、秘密区分指定情報又は要員が開発したソフトウェア・ツールの漏えいに対する監視がある。
- ✧ これらの部隊に関するオープン・ソースの報告は、部隊の創設と一般的な組織構成の概要に限定されている。調査の結果からは、これら部隊の平時における実施内容の詳細に係る要点を示す資料を明らかにすることができなかった。これらの部隊の活動の中心は、CNA 任務に対する緊急事態計画立案を支援するための外国の軍用ネットワークのインテリジェンス収集など、単に軍事作戦要求事項を支援するものと思われる。

任務の細目がどうあれ、PLA は明らかに民間の IT 専門家を継続的に拡大する資源基盤としている。従来からのハッカーは、ある場合にはユニークなスキル・セットを提供し、PLA 又は国家のインテリジェンス収集のすき間を埋める役割を果たすかもしれない。しかしながら PLA は、明らかに、IW を完全なものとするための基盤を民間人 IT 専門知識に

[73] OSC、「PLA の C4ISR 活動総括」、2006 年 4 月 1 日から 5 月 30 日。

期待している。

3.5　中国のハッカー・コミュニティ

中国のハッカーは、数千のウェブ・ベースのグループ及び個人で活動しており、世界中の国々のハッカーと同様に、豊富な知識基盤を開発している成熟した実践者コミュニティであることを示している。これらのウェブ・コミュニティのレビュー結果からは、興味のある多くの階層グループが明らかとなっている。それらは、マルウェア・ツール開発者、正当なセキュリティ研究家、及び訓練を求める初心者や専門家もどきである。これらのグループが投稿するツールや技法は、真のブラック・ハット[74]実践者にしばしば利用されている。

中国のハッカー・コミュニティは、政治的に動機付けされたものであり、外国のネットワークへの大規模なサービス妨害攻撃、データ破壊やハクティビズムと知られているウェブ外観の醜態化を好んで行うことから、早い時期から悪名高きメンバーであるとされている。中国のハッカー・コミュニティは 1999 年～2004 年の間に、外国のネットワークやウェブサイトへの大規模な政治的に動機付けされた攻撃を恒常的に行っていることから、その問題点が明らかにされている。中国のハッカーは、合衆国、日本、台湾、インドネシア及び韓国の仲間とウェブ醜態化や分散サービス妨害攻撃をやり合っており、かつ、中国の法律の免責事項となっていた。このような攻撃は、北京からの有罪宣告がしっかりと条文化されるまではびこっていたのである。彼らの活動は、国家主義の熱情に動機付けされたものの、外国からの中国に対する侮辱的言動に至ることもしばしばであった。ハッカー・グループのリーダーは、彼らのメンバーを統一し、標的を明確にするとともに、多数の参加を確実にするため、攻撃ツールを彼らのウェブサイトを通じて頻繁に普及させた。

- ✧　1998 年 5 月 1 日：インドネシアにおける反中国暴動は、中国ハッカーを刺激して複数のインドネシア・ウェブサイトに対する一連の攻撃を行わせた。
- ✧　1999 年 5 月：セルビアにおける中国大使館への米軍の誤爆のあとを追って、中国ハッカーは、彼らの最初の大規模攻撃をホワイト・ハウスに行った。これは、攻撃計画を立てたメンバーによると、Javaphile グループが率いたとされている。同グループは、「クールな白鳥(CoolSwallow)」という「スクリーン名(screen name)」を用いていた[75]。
- ✧　1999 年：当時の台湾総督 Lee-Teng-hui は、中国により同等の国家として取り扱われるに値するとの意見を述べた。このやりとりに関する西側の新聞報道は、このことが触媒的に働いて大量の中国ハッカー攻撃を引き起こし、台湾国会議事堂、総

74　Black hat：ハッカーのうち、悪意をもってコンピュータやネットワーク攻撃を行う者をいう。

75　Scott Henderson 著、「暗闇の訪問者」、2007 年 1 月、36 頁。

統執務室や多くの政府機関のウェブサイトが攻撃を受けたと述べている[76]。

- ✧ 2001 年 5 月 :「中国の変人同盟(Honker Union of China)」は、合衆国の 1,000 以上のウェブサイトを攻撃したと主張した。この数は、合衆国ハッカーが中国を攻撃したと主張した数にほぼ同じである。これらの攻撃は、合衆国の EP-3 捜索機と中国戦闘機の衝突後に行われたものである[77]。

1999 年～2002 年の間に行われた中国のハッカー・グループが参加した様々な「ハッカー戦争」に対する中国政府の反応は、当初はハッカー・グループを勇気付けるものであり、参加した様々な中国グループの活動を賛美するものであった。しかしながら、2002 年後半以降になるとこの所感が変更され、公式の党のメディアはさらなる大量オンライン活動を思いとどまらせる論説を報じ、いかなる国に対するハッキング活動も不正であり、許されるものではないと示唆した[78]。ハッキング・グループは、国家が今後の攻撃計画に反対するとものであると同論説を解釈し、徐々に身を引くようになった。

- ✧ 2001 年 : ホワイト・ハウスに対する大規模サービス妨害攻撃の後、共産党の公式新聞である人民日報は、同紙のオンライン版に論説を掲載し、中国の攻撃を「ウェブ・テロリズム」であるとして公然と非難した。さらに、「中国の変人同盟」による合衆国のウェブサイトへの攻撃は「法を犯す許されざる行為」であると、効果的に北京の暗黙の了解を撤回させるとともに、ハッカー・グループの組織的運動からの明確な支援を受けて述べた[79]。
- ✧ 外国のネットワークへの大規模攻撃に対する政府の寛容な姿勢が終わりに近づくにつれ、ここ 10 年間の当初に合衆国-中国と台湾海峡横断との間のハッカー戦を行った最も著名な中国ハッカー組織の多くは進化し、専門的な情報セキュリティ・サービスを提供する正式の情報セキュリティ研究会社に変身したようである。これらのグループ又は個人の中には、中国又は政府自身のセキュリティ組織に近い会社との関係を発展させているものもある。

これらの活動に対する政府の姿勢は、精力的な自己検閲制度を創設させるとともに[80]、同様な大規模ハッカー戦の全面的な復活を効果的に抑止させることとなった。しかしながら、グループの中には、対チベット独立などの政治的に「安全」なトピックを共通目的と

---

76 Damon Bristow 著、「サイバー戦は台湾海峡横断に及ぶ」、ジェーン・インテリジェンス・レビュー、Vol. 12、第 2 発行、2000 年 2 月。

77 OSC, CPP20010510000031、「中国ハッカーが中国-合衆国ハッカー戦争の停止を要求」、AFP、2001 年 5 月 10 日。

78 OSC, CPP20010510000031、「中国高官のハッカー攻撃非難についての SCMP 報告」、Vivien Pik-kwan 著、南アジア・モーニング・ポスト、2001 年 5 月 8 日。

79 OSC, CPP20010508000067。

80 Mulvenon 著、「PLA のコンピュータ・ネットワーク作戦」、279 頁。

して呼び集め、今なお外国のウェブサイトに政治的に駆り立てられた攻撃を試みるものもある。

- ✧ 2008 年 12 月 : フランス大統領サルコジが 2008 年にダライ・ラマを訪問した後、ウェブ・グループ「hack4.com」と提携する中国のハッカーが政治的に動機付けされ、合衆国、英連合王国、中国及びカナダのフランス大使館に対するウェブ醜態化を展開した。
- ✧ 2008 年 4 月 : 中国のハッカーによる CNN ウェブサイトに対する大規模な分散サービス攻撃(DDoS)展開の試みは不首尾に終わった。このときに利用したのは、目的をもって構築されたマルウェアであり、一般ユーザーが簡単に取り扱えるものではあるが効果的な攻撃能力を秘めたものであった。この攻撃計画立案は、合衆国の情報戦専門家によって彼のブログ上で明るみになった。そして、この攻撃活動が発信した CNN 向けの多量のトラフィックは、サービス妨害攻撃であるとして、インターネット・セキュリティ分析者達にかろうじて公式に記録された[81]。

国家人民代表会議が 2009 年 2 月に制定した拡大ハッキング法は、ハッキング犯罪に対する一連の目だった逮捕と過酷な刑罰を伴うものであった。これは、おそらく中国のオンライン・ハッカー・コミュニティを対象とした大々的な詳細な調査を行うことで、オープン・オンライン・フォーラムにおける公然のツール交換やハッキング助言を幾分思いとどまらせる可能性があるものと思われる。

- ✧ これ以前の中国の対ハッキング法は、単に中国政府コンピュータ・システムへの侵入を禁止するものであり、厳密には中国のハッカーによる広範なサイバー犯罪行為を置き去りにするものであった。改訂された法には、マリシャス・ソフトウェアの創作と普及に対する取締り条項が追加されている[82]。
- ✧ 治安機関は、既にこの法律をいくつかの目だった素人ハッカーと名声のあるハッカーの両者に適用し、逮捕の上、有罪判決を行った。

---

81 Scott Hendersonの「暗闇の訪問者」ブログ : http://www.thedarkvisitor.com/2008/04/new-kinda-lazychinese-hacker-attack-on-cnn-scheduled-for-tomorrow 及びセキュリティ研究者 Jose Nazario の Arbor ネットワーク上のブログ : http://asert.arbornetworks.com/2008/04/cnn-attacks-inside-two-dedicated-ddostools を参照。Henderson 氏は、最初に攻撃計画に係る議論の脈絡を検知し、CNN に通報した。彼と Nazario の両氏は、彼らのそれぞれのブログ・サイトを通じて議論の進展を常に監視し、CNN システム管理者にアップデートするよう試みつつ、同計画を公表した。

82 「中国の強化されたサイバー犯罪規則」、コンピュータワールド、2009 年 5 月 19 日、次により入手可 : www.computerworld.com/china_toughens_cybercrime_rules。「中国の立法者はハッカーに対し過酷な罰則を考慮」、新華社、2008 年 12 月 22 日、次により入手可 : http://news.xinhuanet.com/english/2008-12/22/content_10544179.htm。「法改定は『愛国的』ハッカーを窃盗や扇動者と同類とみなす」、南中国モーニング・ポスト・オンライン、2009 年 4 月 4 日。

3.6　国家に対するハクティビストの支援

中国の INEW 戦略やその他の IW についての理論や戦略に係る国内文書において、PLA 又は国家安全部がハクティビスト(hacktivist)[83]攻撃を CNO 軍事行動の一構成要素として利用する意図があると示唆するものは少しもない。そして明らかにされているオープン・ソースや一般的なハクティビスト攻撃の大部分の特性上、ハクティビストと INEW 戦略原則との間の両立の可能性はほとんどない。この件に関しての PLA 議論は全く欠如しているか、又はその議論に関する情報源が全く欠如しているものの、このことによって、PLA がハクティビスト攻撃を行うハッカー・グループを雇うことに不本意であるという証拠にはならない。いくつかの要素は、公式の PLA 計画が戦時における CNO 軍事行動の一部としてハクティビズムが含まれることを論証している。

- ✧　**指揮・統制**：全体として、PLA からハッカー・コミュニティに対して指揮・統制機構を難なく取り込めなかったことが、彼らに対する攻撃の指針や指示を極めて困難にしている。ハクティビスト攻撃がいったん開始されると、彼ら自身の勢いを強める可能性があることから、攻撃参加者や攻撃目標に対する統制は、PLA 又は政府機関の能力をはるかに超え、困難なものとなる。また、ハクティビストの自発的な攻撃行動も、PLA 自身のコンピュータ・ネットワーク攻撃を故意でないにせよ混乱させ、機微な CNO 任務とぶつかり合う可能性がある。中国の敵対者に対するハクティビスト攻撃は、PLA がインテリジェンス収集に利用する通信回線を遮断するか、又は PLA 自身のネットワーク攻撃の効果性をモニタするためのフィードバック・ループ通信路の利用を偶発的に壊滅させるリスクがある。
- ✧　**精密標的選定**：INEW 戦略を支配すると思われる中核的原則は、運用に及ぼす影響が最大であると判断された敵情報システムに対して慎重に選定されたノードを攻撃するとした、精密標的選定と規律正しい調整である。その目標は、敵対者の情報のアクセス又は伝達能力に対する支配力を確立することである。ハクティビストの標的選定は、これとは対照的に、一般的に政治的又は国家主義的象徴に基づくものであって、実際の又はハクティビストが認識した PLA 軍事行動目標と一緒になることはない。したがって、PLA の作戦又はインテリジェンス収集活動は、事実上妨げられるおそれがある。伝えられるところによれば、中国のハッカーは 2001 年 4 月の US EP-3 危機の間に、合衆国ウェブ・サーバー上の大量のデータを破壊したとされている[84]。紛争間における合衆国軍のサーバーに対する同様のデータ破壊は、PLA にとって重要なインテリジェンス・ソースを除去するか、又は大規模

---

[83] Hacktivist：hacker と activist（活動家）を合わせた造語である。人権が抑圧や拷問を受ける可能性のあるような地域において外部と通信できるようにする暗号ソフトや匿名通信ソフトなどを開発し、無償配布しているハッカー・グループ活動家の総称をいう。

[84] OSC, CPP20010510000031、「中国ハッカーは中国-合衆国ハッカー戦の停止を要求」、Agence France Press、2001 年 5 月 10 日。

な欺瞞若しくは知覚認識管理作戦の一部として PLA が改ざんしたデータを破壊するおそれがある。また、ハクティビストによる大規模な分散サービス妨害攻撃又は意図的に人目を引こうとするウェブの醜態化は、バックアップ回線を不通にすること、危機解決のための表立った外交努力さえも損なわせること、又は慎重に工作した心理作戦の効果を無効にすることもできるのである。

✧ **徴候と警告**：驚きと欺瞞は INEW 戦略の中核であるが、中国のハクティビスト攻撃は一般的にこの両者とも欠落している。オンライン上の大規模組織は本質的に公共的なものであり、多くのハッカー・グループは、メンバーに対して名目上の審査を行うか、でなければ彼らの議論のスレッド(一連のやりとり)を閉鎖しようと試みるが、そこにはなおもその原因を公にする必要があり、必要であれば標的を公表し、ツールを普及させている。これらの全ては、かれらの計画が検知された上、上手く逆襲される確率を大いに高めることになる。CNN に対する DDoS 攻撃を企てた主催者は、彼らの攻撃予定の変更と一部のウェブサイト変更を行った。このような変更に至った原因の一部は、中国ハッカー・ウェブサイト上の攻撃準備をモニタしていた合衆国に本拠地を置く研究者が、この攻撃を公表し、CNN に警告したことによるものである。

3.7　ハッカーと国家間の協力

中国政府は、CNO ツールの一つとしてハクティビズムを利用することには気乗りしていないように思われるが、スキルの高い人物やハッカー・コミュニティ内の小規模グループとの直接の関係を構築することには意欲があるようである。また、中国政府は、経験豊富なハッカーから構成されている民間会社と契約し、名目上正当な情報セキュリティ・グループとして運用させることもできるようである。このような契約は、ハッカー・ウェブサイト上での政府国防部による簡単な求人広告から、合衆国の政府と民間ネットワークに対する組織的侵入のためのブラックハット・コード開発者による支援に及んでいる。

商用ベースのホワイトハット情報セキュリティ研究者(すなわち、セキュリティ分野における合法的な研究を追及する人達)は、政府顧客を対象としたハードウェアそしておそらくはソフトウェア支援を広く展開している。ここ 10 年間の当初からの最も著名なグループとそれらのリーダーの多くは、解散したか又は一見したところ正当なセキュリティ会社に変身した。Xfocus や Black Eagle Base のような大きなグループは、国家の安全保障と情報セキュリティ目的に密接に連携させたものであったが、彼ら自身を商用ビジネスへと変身させた。

✧ NSFocus は、著名な商用情報セキュリティ会社であり、1997 年～2000 年を通じて活動した著名なハッカー・グループ Green Army Alliance から発展したものであ

る。NSFocus のウェブサイトは、今なお Green Army Alliance のロゴを使用しており、創設者メンバーのリストには最も著名な中国人ハッカーが重要な関係者として名を連ねている[85]。

- ✧ XFocus は、ハッカー・グループから成長した商用の情報セキュリティ会社であり、毎年の Xcon の共同スポンサーとなっている。この Xcon は、NSFocus と Venus Technology がパートナーシップとなっている中国最大の「ハッカー・コンファレンス」である。
- ✧ 河南省の公共治安当局は 2006 年 2 月、The Patriot Hackers-Black Eagle Base のウェブサイトを閉鎖するとともに、そのメンバーを逮捕した。しかしながら、同グループは 6 か月後、Black Eagle Honker Base の名称の下に運用を再開した。同グループのメンバーはこのとき、活動の中心を国家の要員の訓練を行うとともに国家のネットワーク・セキュリティ企業の改善に置く、と主張する声明を行った。このことは、おそらく彼らの釈放条件として、国家当局との協力関係が打ち立てられたことを示唆するものである[86]。
- ✧ また、The Black Eagle の指導部は、国家治安局と国防科学技術委員会(COSTDIN。現在は SASTDIN[87]に改名)に対し、メンバーが拘留中に受けた教育指導に謝意を表明した。SASTDIN は、国防企業政策の監督任務を付与されているが、通常はハッカー・グループ又はその活動に関連して参照付けられることはない[88]。

合衆国のネットワークに対しコンピュータ・ネットワーク・エクスプロイテーションを行った個人又はおそらくグループは、中国の地下又はブラック・ハット・プログラマーが開発したマリシャス・ソフトウェアを取得していた。このカスタム・コードを入手できる能力は、これらのオペレータが地下に潜んでいるハッカー・メンバーを選定するため、何らかのつながりを持っていたことを示唆するものである。

明らかにされた一例として、中国のハッカー・フォーラムに所属するブラック・ハット・プログラマーが 2009 年当初、合衆国の民間会社を攻撃目標にしている侵入者にマリシャス・ソフトウェアを提供したというのがある。フォレンジック分析によれば、このグループ又は個人によって採用された技法とツールは、その前年に同じ会社に対して企てられた侵入時の観察結果と同様のものであることが明らかにされている。

---

85 Scott Henderson 著、「暗闇の訪問者」、29 頁。

86 OSC, FEA20060811026153、「中国は Patriot Hacker ウェブサイトを指導後に復帰させた」、2006 年 8 月 10 日。

87 2008 年 3 月、国防科学技術委員会(Commission on Science and Technology for National Defense: COSTIND)は、再編成されて情報企業技術部(Ministry of Information and Technology: MIIT)の隷下組織となり、現在は国防科学技術国家管理局(State Administration on Science and Technology for National Defense: SASTIND)と名称を変更した。

88 OSC, FEA20060811026153、「中国は Patriot Hacker ウェブサイトを指導後に復帰させた」、2006 年 8 月 10 日。

- ✧ また、このフォレンジック分析は、このグループが様々なスキル・レベルをもった複数メンバーから構成されていたこと、定められた予定と標準運用手順に従って行動していたこと、及び標的となったコンピュータ上の活動を隠すため好んで詳細なステップを踏んでいたことについても示唆している。
- ✧ 2009 年当初に利用されたマルウェアを創ったコーダーのスクリーン・ネームに係るオープン・ソースの調査の結果、当該人物は中国生まれの話し手であり、EvilOctal として知られている著名な中国ハッカー・グループ・ウェブサイトの論議掲示板に、ルートキット付のキーストローク・ロギング・プログラムを掲載していたことが明らかとなった。
- ✧ そのコーダーは、ツールと一緒にマリシャス・ソフトウェアの伝染を目的とした添付資料に利用する PDF 文書を作成したが、これは中国語だけで利用できるものであり、FreePic2Pdf、1.26 版と名付けられていた。この文書は、Adobe Acrobat の未知ぜい弱性を標的にしたゼロデイ利用を密かにインストールするため、改善されたものである[89]。
- ✧ ユーザーが添付資料を開け、犠牲となったシステムにうまくインストレーションが完了されると、トロイの木馬マルウェアが定期的に海外の他のマシンとの接続試みを開始する。そして、マシンへの攻撃がうまくいったことを攻撃者に知らせるための合図を伝送する。侵入者は、犠牲となったコンピュータとの暗号化通信を介し、次のフェーズ開始準備ができたときだけ、この接続を利用する。
- ✧ オペレータは、24 時間 3 シフトのサイクルで作業し、前の攻撃で観察されたものと同様の偵察コマンドを出す。
- ✧ そして、このコンピュータと以前危殆化した同一ネットワーク上のシステムとの間にかなり大きな違いが認められると、攻撃チームは少量のデータを抽出して、インストールされたセキュリティ・ソフトウェアのコンフィギュレーションを調査するとともに、会社ネットワーク上の攻撃目標データに対する彼らのアクセス能力をチェックする。
- ✧ オペレータは、検知されることなく犠牲となったコンピュータへのアクセス特権が攻撃者に提供されるよう、ルートキット[90]をインストールした。これは、攻撃者の意図が、長期間に及び犠牲となったコンピュータを密かに利用するものであることを示唆している。攻撃者は、ルートキットを設定し、次のシステム・リブート時に実行させ、オペレータのファイル、プログラム、ネットワーク接続及びレジスト

---

89 このぜい弱性についての詳細は次により入手可：
http://www.adobe.com/support/security/advisories/apsa09-01.html 及び
http://www.kb.cert.org/vuls/id/905281

90 rootkit：コンピュータ・システムへのアクセスを確保した後で、第三者(侵入者)が使用するソフトウェア・ツールをいう。

リ設定を効果的に隠そうとした。しかしながら、オペレータのエラーがルートキット実行上の問題をもたらし、攻撃者は犠牲となったコンピュータから閉め出され、活動が終了した、とフォレンジック分析結果は述べている。

- ✧ ルートキット・コードは、未だおおっぴらに入手できるものではない。このことは、攻撃者がコーダー自身又はその人物に直接アクセスできる誰かから直接入手したことを示唆するものである。

この他の 2008 年秋に合衆国の会社攻撃に利用されたゼロデイ・エクスプロイトの作成者は、中国語とデフォルト言語として中国語設定のマシン上でそのコードを開発した。このことは、この人物が中国生まれか中国語に達者な者と思われることを示している。フォレンジック分析結果からは、この他に開発者のアイデンティティに係る詳細を入手することができるものはほとんどなかった。しかし、上記は、中国のブラック・ハット・プログラマーと合衆国のネットワーク侵入に責任がある個人との間に、関係があったとする主張を強化するものといえる。

- ✧ 合衆国の会社がスパムもどきの E メールの小さな波を受け始めた。このメールの添付資料には Microsoft WordPad(.wri)ファイルがあり、マリシャス・ソフトウェアの小片が含まれていた。このマリシャス・ソフトウェアは、トロイの木馬として活動し、攻撃者に標的となったコンピュータへの完全なアクセスを可能にするものであり、折り紙付の中国製コンピュータ・ネットワーク・エクスプロイテーションのスパイ技術である。このマルウェアは、Microsoft WordPad アプリケーション内のゼロデイぜい弱性をエクスプロイトしたものであった[91]。
- ✧ これらの E メール攻撃で送付された添付資料には、2 つのコンポーネントが含まれていた。一つは、英語の文書であり、防衛関連企業が下請負契約者を利用する際の一般的な契約書式と思えるものであった。もう一つは、同文書内に挿入された中国語のエクスプロイト・コードであった。
- ✧ スパムらしい E メールの受取人が添付資料の.pdf ファイルを開けようとすると、そのファイルは、次にユーザーがログインした際に実行するように仕組まれたマルウェアとバックドア・サービスの両者を標的マシンにインストールした。

スピア型フィッシング攻撃の波により、様々な合衆国会社に対し送付されたマルウェアは、侵入者が標的となったコンピュータをリモートからアクセスし、制御できる機能が仕組まれていた。この他の一般的なコンピュータ・ネットワーク・エクスプロイテーション活動の特徴は、中国に起因すると思われるものであった。

---

91 マイクロソフト・セキュリティ助言 960906 を参照。

✧ 新たにインストールされたサービスは、標的となった会社のネットワーク外の外部ホストに接続し、同じアクセスと運用機能でもって、あたかも侵入者がユーザーのキーボードの席に座っているかのようにリモートから犠牲となったマシンを制御できるようにする。

2008 秋の攻撃行動間に利用されたマルウェアのプログラミング・バグ、及び取り換えプログラムとして初期のバージョンを迅速に入手できる侵入者の能力は、これら攻撃者に新たなバージョンが最初に利用されたことを強く示唆するものであった。取り換えバージョンを迅速に入手する彼らの能力は、その開発者又は開発者の製作物リポジトリを管理している誰かにアクセスできた結果であると思われる。仮に、後者が真実であるとすれば、合衆国政府と商用のネットワークに攻撃を行う者に対して、支援インフラが存在することをほのめかすものである。とはいえ、このことは今なお憶測にすぎず、確証するにはさらなる調査が必要である。

✧ マルウェアの初期バージョンは、2008 年 10 月末にコンパイルされ、一週間以内に侵入者に利用された。製作完了と最初の利用の間がこのように短期であることは、侵入者(又は侵入者達)がカスタマイズされたゼロデイ・マルウェアを迅速に入手する手段を持っていることをほのめかすものである。
✧ 侵入者がコードに運用上の問題に遭遇すると、その侵入者は即座に 2008 年 1 月にコンパイルされた古いバージョンのマルウェアを入手し、若干の遅れで攻撃を再開した。

3.8 ハッカー・グループからの政府採用

中国ハッカー・コミュニティの中から政府職員を採用するとした政府の活動、及び有名なハッカーやセキュリティ･サービスと政府との間のコンサルティング関係の証拠からは、これらの専門家集団から情報を引き出すとした政府の何らかの意欲をほのめかしている。しかしながら、このことは、当局がこのような関係を多く打ち立てたとか、又は合衆国のシステムに対する大規模攻撃を仕掛けるため、これらのグループに協力を要請する政府の意図を意味するものではない。

✧ 2007 年 7 月～2008 年 11 月の間、スクリーン・ネーム「City_93」を利用している人物が、EvilOctal.com と XFocus.net の掲示板（www.fri.com.cn）に中華人民共和国公安部第一研究所の求人案内を掲載した。この EvilOctal と XFocuse は、中国におけるハッカー・フォーラムであり、とりわけ XFocuse は最も確立されたものとして知られている。
✧ 「City_93」は結局、2007 年から 2008 年の間に 10 件の求人告示を EvilOctal に

掲示し、両サイト上で応募要領と職務内容の性質について長ったらしい論議を繰り返した。その求人掲示板は、ネットワーク・セキュリティ・システム・プロジェクトの開発と実施経験を持つ初心者レベルのプログラマーに対するものであった。

✧ 公安部第一研究所は、公安部の運用部門に対し様々な科学技術研究開発を行っている。同研究所のウェブサイトによれば、情報セキュリティ研究グループが研究所内にあるとされている。

図 4：公安部第一研究所代表者によるハッカー・ウェブサイト EvilOctal 上の求人案内

図 4 は、情報セキュリティ及びプログラミング経験者の求人案内である。この掲示は、スクリーン・ネーム「City_93」のユーザーによって行われたものであり、彼自身は公安部の職員であると自ら名乗り、公安部の E メールを以降の連絡に利用している。

学界出版物と報道及び本調査とは別個の IW 分析家の分析結果によれば、大きな影響力を持つ中国ハッカー・グループ Javaphile の創設者メンバーは、上海公安局と公式のコンサルティング関係にあるとともに、中国のある一流大学の情報セキュリティ・エンジニアリング研究所における研究者資格を持っているとされている。Javaphile は、ハクティビスト・グループとしての確固たる経歴の持ち主で、2001 年～2002 年におけるホワイト・ハウスやその他のネットワーク攻撃を率いたことで知られており、今なお大きな影響力を与える活動グループであると考えられている。

- ✧ Javaphile の共同創立者である Peng Yinan は 2003 年、上海膠南大学の学生オンライン・フォーラム上にスクリーン・ネーム「CoolSwallow」を用い、彼が膠南大学の情報セキュリティ・エンジニアリング課程に在籍していた 2000 年に、Javaphile を創設したと投稿した。その投稿は、それ以来取り除かれている[92]。Javaphile グループは当初、ジャバ言語ユーザー・グループとしてもっぱら活動していたが、EP-3 インシデントの発生がグループ・メンバーに大きな変化をもたらし、Javaphile をハッカー・グループに変身させた。同メンバーは、ツールの開発、技法の共有、及び合衆国ウェブサイトへの攻撃実施を活動の中心とした、と同グループによる上海膠南学生オンライン・フォーラムへの投稿が示している[93]。
- ✧ 合衆国 IW 専門家 Scott Henderson による別個の調査では、Peng を 2 つのスクリーン・ネーム、CoolSwallow と Ericool に結び付けている。この 2 つは、彼が頻繁に利用したスクリーン・ネームであり、彼の Javaphile ウェブサイトや別個のウェブサイト上の仏教に係るエッセイ稿のどちらにも利用したネームである。この別個のウェブサイトは、仏教テーマ専用のものであり、Peng はそのメンバーであった。
- ✧ Henderson は後に、Peng の上海公安局コンサルタント資格を上海膠南大学の学生新聞記事から明らかにした。この記事は、情報セキュリティ・エンジニアリング課程卒業生である Peng による学生への講義ついて記述したものであり、そのときの演題は「極めて簡単なハッカー」であった。これらの記事及び公共の掲示版においても、Peng を「経験豊富なハッカー」とした解説を付記している(図 5 参照)[94]。

  図 5 は、Peng Yinan が 2007 年に上海膠南大学で行った講義「極めて簡単なハッカー」の宣伝ポスターである。彼の名前は、円に囲まれており、彼のハッキングと公安部資格には下線が引かれている[95]。(訳注：不思議なことに、この線は、原文では表示されているものの、本原稿を作成する際のコピー後に消えた。彼の名前や所属は、同図左下の部分に掲載されている。「上海市公安局情報セキュリティ顧問」と掲載されている)
- ✧ Henderson のブログでこの暴露が行われた後、CoolSwallow と Buddhist の両クラブ・サイトはこきおろされ、オンライン・ハッカー・フォーラムでは一年間に及び CoolSwallow 又は Ericool についてお目にかかることはほとんどなかった。

---

92 CoolSwallow、Ericool 及び Peng Yinan 間の結びつきについての完全な分析については、Scott Henderson の分析と彼が自身のブログに掲載した研究成果を参照されたい。「暗闇の訪問者」は次により入手可：http://www.thedarkvisitor.com/2007/12/javaphile-buddhism-andthe-public-security-bureau/

93 Scott Henderson 著、「暗闇の訪問者」、2007 年 4 月、36 頁。

94 Scott Henderson 著、「暗闇の訪問者」ブログ。上海新聞の記事は、次により入手可：http://jd.sjtu.edu.cn/BKPG/xsyd/xywh/2007-11-05/1194245625d7507.html

95 次を参照：http://jd.sjtu.edu.cn/BKPG/xsyd/xywh/2007-11-05/1194245625d7507.html

図 5：Javaphile メンバーと公安局コンサルタントの宣伝ポスター

- ✧ Peng はその後の 2008 年に、コンピュータ・ネットワーク・エクスプロイテーション技法に係る 2 つの論文を、彼自身の氏名と上海膠南大学情報セキュリティ・エンジニアリング研究所所属を明示して出版した[96]。
- ✧ 同研究所は現在、Peng Dequan が長となっている。彼は、中国の主要なインテリジェンス機関である国家安全部科学技術委員会の元委員長でもあった[97]。

台湾のメディアは、裏付けはとられていないものの、四川大学学生新聞からの記事を参照して次のように報じている。「伝えられるところによれば、PLA は 2005 年に一連の行政地区又は省レベルのハッカー大会を開催し、軍の CNO 要求事項を支援することができる能力のある市民を明らかにした」

---

96 この 2 つの論文の題名は「ブラインド SQL インジェクション技法の分析」及び「インジェクション投入と Web 2.0 の防衛」であり、「情報セキュリティと通信セキュリティ」雑誌に出版された。この雑誌では、Peng と共著者（以前の Javaphile メンバーでもあった）を、上海膠南大学情報セキュリティ・エンジニアリング研究所所属の研究者としていた。出典は Wanfang データベースであり、次により入手可：http://d.wanfangdata.com.cn/Periodical_xxaqytxbm200805032.aspx

97 「コンピュータ・セキュリティの厳格化が急務」、PLA 日報オンライン、英語版、2000 年 8 月 14 日、次により入手可：http://english.peoplesdaily.com.cn/english/200008/14/eng200008_48117.html。CPP20060908425001001、「武漢大学をソフトウェア・エンジニアリング主要研究所に指定」、2006 年 8 月 28 日。

- ✧ 中国のハッカーWithered Rose(枯れたバラ)(別名：Tan Duilin)、つまり著名なNCPH ハッカー・グループの元リーダーは、四川大会において優勝したと伝えられている。この記事は西側のメディアにしばしば繰り返し報告されているが、その詳細を確認するのは困難である。
- ✧ 同記事は、四川軍指揮通信部が 2005 年、明らかに Tan に直接接触し、省軍事司令部が開催するネットワーク攻撃と防衛訓練に参加するよう求めたとしている。これは、同年後半に行われた成都軍指揮ネットワーク攻撃と防衛大会の準備のためであったと、Tan にインタビューした四川大学科学技術学生新聞は述べている[98]。仮にこの記事が真実であるとすれば、PLA がハッカー・コミュニティ内での「タレントのスカウト」や、活動を推進するこの大会のような公式行事の組織化に取り組んだことをほのめかすことになる。
- ✧ 最近、Tan がライバルのハッカー・グループのウェブサイトを攻撃したとして逮捕されたことは、極めて興味深いことである。

3.9 政府のコンピュータ・ネットワーク作戦と研究開発に対する民間の支援

中国の長期に及ぶハイテク・セクターへの投資は、実を結びつつある。これにより PLA は、C4ISR やコンピュータ・ネットワーク作戦(CNO)の要求事項に係る支援を民間から受けるため、ますます増加する多くの先進 IT システムの設計、構築及びサービスが可能な国内会社にアクセスすることができるようになった。これらの従業員を民兵部隊にリクルートできることは、政府が中国の IT セクターの発展から引き出す一つの利点でしかない。Huawei 社など、会社の中には西側でもよく知られ、中国と海外両者における相当のマーケット・シェアを占めている会社もある。とはいえ、Venus Technologies 社などその他多数の小規模会社も、PLA と政府の治安組織にますます精巧なプラットフォームや技術を提供している。

- ✧ Huawei 社は、PLA に十分認められた特殊電気通信装置、訓練及び関連技術のサプライヤーであり、Zhongxing や Datang などの他の会社と共に、C4ISR システムの戦闘能力に係る研究開発予算を直接支給されている。これら会社の全ては、国家研究機関として発足され、PLA からの優先的予算と支援を継続して受けている。[99]
- ✧ 中国における他の大規模電気通信製造会社である ZTE Corp と Huawei は、通信

---

98 OSC, CPP2007111531000、「Tzu-Yu Shin-Pao：中国は 30,000 人のインターネット兵士を採用」、2007 年 11 月 10 日。Simon Elegant 著、「ファイアウォールの敵」、Time Magazine、2007 年 12 月 6 日、次により入手可：http://www.time.com/time/magazine/article/0,9171,1692063,00.html。

99 Evan Medeiros、Roger Cliff 及び Keith Crane 共著、「中国の防衛企業の新たな方向」、RAND 会社、2005 年、213 頁。

と IW 関連職務に配置された PLA 要員に対する資格取得のための訓練及び関連するエンジニアリング訓練を提供している、と省レベルの共産党軍事新聞が伝えている[100]。

- ✧ 民間 IT 会社は、IW 民兵部隊充足のための要員を派遣している。同民兵部隊には、戦時における CNA と CND の両任務、及び平時における広範囲に及ぶ CNE 任務が付与されている[101]。
- ✧ Venus Technology Inc.は、ハッカー・グループ XFocus 及び NSFocus と密接な連携関係にあるが、多くの PLA と中国政府機関組織に対する情報セキュリティ及びコンピュータ・ネットワーク作戦専門家のプロバイダーとしてもよく知られている。Venus のウェブサイトに掲載されている顧客リストの中には、全 PLA 軍、全参謀部(すなわち、総参謀部、総政治部、総後方勤務部及び総装備部)と中国北部企業グループ(China North Industries Group: NORINCO。十分な資料の裏づけがある兵器輸出業者)防衛企業協会、中国航空機産業組合(Aviation Industry Corp: AVIC)、中国航空宇宙科学技術グループ(China Aerospace Science and Technology Group: CASTG)、中国造船産業組合、及び内モンゴルに設置された中国の最も古い宇宙打ち上げ施設である酒泉人工衛星打ち上げ基地が含まれている[102]。

今日に至るも、PLA やその他の国家治安グループが中国ハッカーを利用して、合衆国のネットワークに対してコンピュータ・ネットワーク・エクスプロイテーションを実施したとする関連証拠の記録は、極めて間接的なものである。中国政府が「インターネット陸軍」を多数の中国ハッカーからリクルートしたと主張する西側のメディア報告は、怪しいものである。しかしながら、オープン・ソースから入手できる報告は限定されているものの、それらは、国家治安組織が洗練されたハッカー・スキル・セットを持つ人物からコンピュータ・ネットワーク作戦専門知識を求めているとした、いくつかの前例が存在することを強く示唆している。これらの組織は、リクルートした人物をどのように利用しているのであろうか、どのような国家主催の CNO 活動にどれくらいの数の人物が参加しているのであろうか、そして、いったい、これらの人物が現在行われているサイバー・インテリジェンス作戦にどのように統合されているのであろうか、これらの全ての解明には十分な吟味と継続した調査研究が必要である。

---

100 OSC, CPP20090430682010、「ネットワーク『スパイダーマン』－ある主要通信所の NCO 第 6 級 Wang Jianquo 回想録」、Gong Yun、Xia Hui 及び Zheng Xisheng 共著、広州 Zhanshi Bao、2009 年 3 月 5 日、4 頁。

101 OSC, CPP20031002000138、「高品質民兵情報技術小隊の構築」、Ye Youcai 及び Zhou Wenrui 共著、PLA 広州守備隊区、軍事科学院、Guofang、2003 年 9 月 15 日。

102 この顧客リストは、次に示す Venus Tech のウェブサイトから入手可：http://www.venustech.com.cn/aboutitem/189。

4　サイバー・スパイ[103]

外国のインテリジェンス機関は、以前手が届かなかったか又はそれを入手するには数年に及ぶ高価な技術的若しくは人的資産の用意が必要であった非秘密区分指定の合衆国政府及び民間セクターの情報であても、コンピュータ・ネットワーク作戦用ツールを利用することによって、比較的簡単にアクセス、検索及び窃盗が可能であることに気付いている。機微な合衆国情報に対してこの方法で標的行為に及ぶ場合、現在の投下資本利益率（インテリジェンス利得）は驚くほど高くなっており、かつ、侵入時の障壁（作戦遂行に必要なスキルと技術）は比較的低いのである。多くの国々は、この脅威に防衛的に対抗するため、その能力の開発プロセス中にあるか、又は彼ら自身の攻撃的ネットワーク作戦プログラムを構築しているかのいずれかである。しかしながら、中国は、メディア報告に指摘された大部分の活動の陰に隠れた主要な活動家であるとして最も頻繁に引用されている。そして合衆国当局は、中国のネットワーク・エクスプロイテーション及びインテリジェンス収集活動が合衆国にとっての最大のカウンターインテリジェンス課題の一つであると、公言してはばからない状況にある。

中国のコンピュータ・ネットワーク作戦能力の開発は、戦時における作戦準備をはるかに超えたものである。PLA と国家治安組織は、合衆国や世界中の多くの国々に対するインテリジェンス収集目的で、大規模なコンピュータ・ネットワーク・エクスプロイテーション活動を行うためにこの能力の採用を開始したということが、合衆国当局の声明発表、標的にされた外国政府の非難、及びこれらインシデントを報告するメディア組織の増加によって明らかにされている。

コンピュータ・ネットワーク・エクスプロイテーション技法を利用し、合衆国政府及び合衆国防衛企業からの機微ではあるが非秘密区分指定情報を収集するとした長期に及ぶ継続した組織的活動は、以前から中国が関与したものと考えられている。そしてこれにより、2007 年において少なくとも 10～20 テラバイトのデータが、合衆国政府のネットワークからこっそりと首尾よく持ち出されたと、合衆国空軍は推定している。過去の数値は公表されていないものの、考えようによっては、過去 2 年間で急速に増大したと思われる。

---

103 以下の節の内容は、メディアの分析結果によるものであるが、またノースロップ・グラマン社が保有する深い知識と洞察力にもよっている。当社は、それらを情報セキュリティ・サービス・プロバイダーとしての実績、及び地域的に分散配置されている当社の大きな組織の防衛経験に基づき獲得したものである。ノースロップ・グラマン社の合衆国に向けられたサイバー脅威の特性に対する理解は、深い、現実世界の経験に基づくものである。さらに、ここに示したインシデントや洞察は、オープン・ソースによる調査と当社全体としての様々な先進サイバーセキュリティ問題を論じる成熟度によるものである。**本調査において示すインシデントと敵対者の行動パターンは、明確に指定しない限り、いかなる特定の会社又は政府機関について言及するものではない。**

James Cartwright 将軍は合衆国戦略軍の戦闘指揮官として勤務していたとき、議会の委員会において、中国は、民間会社は無論のこと、合衆国政府機関のコンピュータ・ネットワークをプロービングすることにより、実際にサイバー偵察を行っていると証言した。彼はさらに、これらのコンピュータ偵察行動から収集したインテリジェンスが無数の目的に利用され、それらにはネットワーク中の弱点を明らかにすること、合衆国のリーダーがどのように考えているか理解すること、アメリカ政府機関と民間会社の通信パターンを発見すること、及びネットワーク中に保管されている貴重な情報を獲得することが含まれると言及した[104]。

合衆国そしてますます世界中の多くの国々に対するこれら組織的活動全般の規模、焦点及び複雑に対する調査の結果からは、これらの活動が国家の後援又は支援の下に行われていることを強く示唆している。オペレータは、金融、人事及び分析資料にアクセスしているようであるが、それらの活動規模は、これまでの数年間に組織犯罪活動やそれぞれ独立に活動している複数のハッカー・グループが行ってきた同様のアクセスをはるかに超えるものである。さらに、盗まれたデータの種類は、サイバー犯罪組織が主な窃盗対象としたクレジット・カード・ナンバーや銀行口座情報のような金銭的価値を伴うものと本質的に異なるものである。高度の技術的防衛エンジニアリング情報、軍事関連情報、又は政府政策分析文書は、顧客が国家でない限り、サイバー犯罪者がそれらを金銭に換えることはできないものである。このことは、キーボードを操作しているオペレータの所属にかかわらず、その活動が「国家の後援の下」に行われていることを欠席裁判により決定付けるものである。

彼らの活動範囲と標的としたネットワークに関する深い知識、及び盗み出されたデータの量と項目内容からは、防衛関連エンジニアリング研究に参画している者、米中関係に関心のある政策専門家、及び合衆国の軍事情報システムとその運用に係るインテリジェンス収集計画を立案する軍の関係者を、攻撃者が支援していることを示唆するものである。

合衆国政府当局は、全体として、この活動が合衆国の長期に及ぶ科学技術の革新と競合性における世界のリーダーとしての位置づけを損なわせる可能性があるとともに、合衆国防衛エンジニアリング・データが受取人側の研究開発期間の短縮化と相当な予算削減をもたらしたのではないか、と判断している[105]。

---

104 「中国軍の近代化とそれが合衆国とアジア太平洋に及ぼす影響」、米中経済安全保障調査委員会での聴聞会、2007 年 3 月 29 日～30 日、7 頁、次により入手可：
http://www.uscc.gov/hearings/2007hearings/transcripts/mar_29_30/mar_29_30_07_trans.pdf

105 Jeff Bliss 著、「中国のスパイ活動は合衆国カウンターインテリジェンスを圧倒」、Bloomberg、2007 年 4 月 2 日。Shane Harris 著、「中国のサイバー民兵」、The National Journal、2008 年 5 月 31 日土曜日、次により入手可：http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php

これらの活動はある程度成功している。その理由は、現在の企業及び合衆国政府の情報セキュリティ・パラダイムのほとんどが、たいていは先進攻撃に対して不適切な従来からのシグナチャー・ベースの対ウィルス・ベンダー・モデルや一般的なホストとネットワーク防衛対策などに基づいているからである。製品ベンダー又は研究コミュニティが新たなセキュリティぜい弱性を開示すると、セキュリティ・ソフトウェア・ベンダーが速やかにそれを分析し、「シグナチャー」又はこの新たなぜい弱性攻撃に伴い予測される影響の説明書を作成する。これらのシグナチャーは、侵入検知/予防システム(Intrusion Detection and Prevention System: IDS/IPS)やファイアウォールなどのネットワーク制御装置、及びウィルス対策ルールとして個々のコンピュータ又はホストの IDS/IPS に適用される。ぜい弱性に関する事前の知識なしに又は研究所の攻撃例を見ないで、率先してこれらのシステムにシグナチャーを追加することは困難であり、たいていはやる気を失わせるものである。

- ✧ 多くの組織は、エクスプロイトが公にされていないぜい弱性に対してシステムやソフトウェアにパッチするのは気が進まないものである。より成熟したセキュリティ慣行又は資源がある大きな組織では、たいていはセキュリティ・イベントと情報管理(System Event and Information Management: SWIM)又はネットワーク行動分析(Network Behavioral Analysis: NBA)に適用される複雑な行動のシグナチャー又はモデルを利用しているが、これらの技法は一般的にコンポーネント・シグナチャー・ベース・システムから提供されるものであり、これらもまた、同様の欠点による痛手を被ることとなる。
- ✧ NBA システムは、変則的な行動を探すように調整された場合、大きな将来性がある。とはいえ、このモードでは、一般的にはさらなる管理上のオーバーヘッドと誤警報率をもたらすことになる。
- ✧ 従来のネットワーク及びシステム管理は、性能、出費とセキュリティの均衡化であり、一般常識的には活動中のシステム、たいていは重要なシステムの変更を行うことにある種のためらいを感じさせている。

これらのオペレータはこの反応性の防衛モデルを利用するのであるが、彼らは予め未知のぜい弱性を明らかにして利用するための十分な資源を持っている。この未知のぜい弱性は、シグナチャー・ベースの IDS/ISP とエンドポイントの防護ソフトウェアがよく見過ごしてしまうものなのである。中国の学界とハッカー・グループは、世界中の多くのハッカー・グループと同様に、新たなゼロデイぜい弱性の調査活動に焦点を当てているのである。

- ✧ 情報セキュリティ企業ソースからの間接的な報告によれば、確証付けられてはいないものの、中国の研究家も好んで第三者組織からゼロデイ攻撃ツールを調達して

いることを示唆している。

- ✧ ゼロデイ・エクスプロイトは、犠牲ソフトウェア・ベンダーと何らの掛かり合いもなく、無数の公共及び私的市場において売買されている。時には、一ぜい弱性あたり何万ドルもするのもある[106]。

今日に至るまでの全般的な活動は、活動のテンポが速いことと広範な標的行為が観察されていることから、複数のグループとスキルのある個人によって構成され、それぞれが異なる標的に対して活動を行っているものと思われる（中国による侵入と言われている対照年表については下記を参照）。これらのオペレータは、ある者は中国政府又は軍組織に所属していると思われ、その他はおそらくフリーランスのハッカーであろうが、ゼロデイ・エクスプロイト開発能力があるソフトウェア・ベンダーへのアクセス権を持ち、たいていは中国語設定のコンピュータ又は中国語デベロッパー・キット上で作成されるツールを利用する者である。

- ✧ この件に関連する敵対者の活動は、成功裏に終わっている。なぜなら、彼らは攻撃目標のネットワーク上に長期間滞在することが可能なことから、ネットワーク・トポロジーの偵察、高価値情報のあり場所の決定、将来のスピア型フィッシング行動を支援する専門的なネットワーク分析などを行い、運用上の活動が必要になった時に危殆化されたコンピュータへの接続を速やかに確立することができるからである。
- ✧ スピア型フィッシングに係る情報は、一般的には現在のプロジェクトや受信者が出席した会議を参照して具体的で正当と思える E メールを作成し、標的にされたユーザーに伝送するためによく利用される。この E メールには、一般的に添付資料にマリシャス・ソフトウェアが組み込まれているか、又は悪意のあるウェブサイトへのリンクが含まれている[107]。
- ✧ この活動に関連した標的行為の規模と複雑さは、おそらくオペレータ、インテリジェンス分析家やマルウェア開発者などの多様なチームに対して、優先順位を整理して伝達することができる成熟された収集管理組織によって支えられていることを示唆するものである。これらの人物は、制服の軍人、文民のインテリジェンス・オペレータ及びフリーランスの高級ハッカーの混成と思われる。

これらの種類の攻撃は、たいていEメール・メッセージで開始される。このEメールに

---

106 例は次により入手可：http://www.securityfocus.com/columnists/470。さらなる背景については次により入手可：http://www.eweek.com/c/a/Security/Hackers-Selling-Vista-ZeroDay-Exploit/。

107 Brian Grow、Keith Epstein 及び Chi-Chu Tschang 共著、「新たな E スパイ脅威」、BusinessWeek、2008 年 4 月 10 日、次により入手可：
http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

は、エクスプロイト・コードと犠牲となったコンピュータの制御を攻撃者が行える別のソフトウェア小片が組み込まれたファイルが添付されている。このファイル(たいていはイメージ・ファイル)、文書又はスプレッド・シートが犠牲となったコンピュータ上のぜい弱性のあるプログラム(例：Powerpoint、Wordpad、Adobe Acrobat など)によってオープンされると、バックドア・プログラムが実行される。E メールは最も一般的なエントリ・ベクトルである。なぜなら、オペレータは、一般的に従業員(又は従業員グループ)の信頼関係(すなわち、かれらの職業的ネットワーク)を、誰が頻繁にメールしているのかを分析することで知ることができるからである。そこで、侵入者は、信頼できると思われるような E メールを、ネットワーク中のメンバー又はグループから作成するのである[108]。

図 6 は攻撃 E メールの一例であり、多くの合衆国の会社に同時に送られたものである。関連する情報やカンファレンスは原文を変更したものである。

日付：2008 年 12 月 10 日、火曜日。06:58:13-0700(PDT)
送信者：John Doe<john.q.googdguvy@yahoo.com
宛先：従業員。氏名＠社名.com
件名：第 7 回年次合衆国防衛カンファレンス、2009 年 1 月 1-2 日

場所：ワシントン DC のロナルド・レーガン・ビル及び国際貿易センター

2009 カンファレンス予備プログラム(PDF)のダウンロード
http://conference.satellite-stuff.net/events/MDA_Prelim_09.zip

2009 カンファレンス登録申込書 (PDF)のダウンロード
http://conference.satellite-stuff.net/events/MDA09_reg_form.zip

連絡先：John Doe
情報システム契約者
(703)555-1234
john.doe@yahoo.com

図 6：攻撃 E メールの一例

図 6 に示す E メールの一例において参照付けられたカンファレンスは正当なものである

[108] Brian Grow、Keith Epstein 及び Chi-Chu Tschang 共著、「新たな E スパイ脅威」、BusinessWeek、2008 年 4 月 10 日、次により入手可：
http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

が、ダウンロード先のリンクはそうではない。登録申込書とプログラム・ファイルは、ダウンロードし、アンジップすると、攻撃者に標的とされたユーザーのコンピュータの完全な制御権を与えてしまうことになる。標的行為任務を遂行するオペレータは、予めこの会社の従業員と他の全ての受取人を明らかにしている。なぜなら、この E メールの件名に関心を持ち、かつ、登録申込書をダウンロードすると思われる従業員について、オンライン上でその所在を明らかにしているからである。オンライン上とは、カンファレンス出席者リスト、ニュースグループ(インターネット上の分野別情報提示サービス)、Facebook や Linkendin などのソーシャル・ネットワーキング、会社の公開情報などである。

- ✧ オペレータは、この偵察活動によって得られた従業員のプロフィールを、複数標的行為の企てにしばしば再利用する。なぜなら、当該ユーザーが最初のときは添付資料を開くのを怠った人物か、又は単に彼らが「だまされやすい人」でたいていはこれらの E メールをオープンしてしまう人物であることから、侵入者にとっては信頼できるエントリ・ベクトルになるからである。
- ✧ この E メールと悪意のある添付資料による侵入開始は、先進的活動の最初のフェーズにしかすぎない。なぜなら、最初に標的にされたユーザーとそのコンピュータ上のデータは、たいていは実際の収集標的ではないからである。攻撃者によるデータ所有者を標的にした実際の収集行為は検知されるリスクを高めるものであり、攻撃者が持ち出そうとして探し求めているデータについてはより厳格な制御が行われていると思われる。したがって、攻撃者による後段の収集行為の企ては、より困難なものとなる。

国家が後ろ盾となった洗練されたオペレータが関与した侵入に係るフォレンジック・データ分析の結果は、侵入活動に複数の人物が参画していると思われものもがあったことを示唆している。それらの人物は、ネットワーク・アクセスの入手と確立を行う者、価値のある情報を明らかにするために標的にされたネットワークの一部を捜索する者、及びデータの持ち出しについて計画準備を行う者としての責任がそれぞれ付与されていたものと思われる。エントリ又は「突破チーム」という役割は、エントリを入手し、標的としたネットワークにおいて柔軟かつ冗長性のある存在を維持する任務が付与されるだけである（本質的には「開錠」であり、ドアを確実にオープン状態に維持するだけでなく、利用中のドアが「閉鎖」された場合に備え複数のドアを利用できるようにしておく)。いったん突破チームがネットワークへのアクセスを首尾よく確立すると、第二のチーム又は人物がデータ偵察を行い、最終的には標的となるデータの所在を突き止め、持ち出すことになる。

別の人物又はグループを利用する理由は、侵入の各フェーズにおいて必要な特殊技術によるものか、又は「区画化」の理由によるものと思われる。区画化については、第一のチ

ーム又はオペレータは、第二のチーム又はオペレータが何を標的にしているか、その詳細を知る必要がなく、このようにすれば、理想的には活動全体のセキュリティを改善することになるからである。しかしながら、このようなエクスプロイテーションは、ほとんど推論にすぎない。なぜなら、これらのインシデントに係るデータは、侵入の背後に存在する実際の要員の内部通信、識別又は力学関係を明らかにする情報を提供することは決してあり得ないからである。

- ✧ この種の任務指向の構成は、おそらくある活動を遂行するに当たって何人かの人物からなる複数のスキル・セットを必要としている。仮に、このモデルが正しければ、このようなチームの採用、組織化及び管理のための手段が必要になると推察できる。仮に、このモデルが本当に正確で、これまでの多くの侵入に繰り返されたとするならば、監督機構はそれなりに大きくかつ複雑でなければならない。
- ✧ いったん突破チーム又は個人が最初の犠牲コンピュータ上の足場をセキュアな状態に保つと、彼らはこのマシンのセキュリティ・コンフィギュレーション、設定状況、及び関連するシステムに係る情報収集を継続し、彼らの存在を確固たるものにする。時には、認可システムからパスワードを検出し盗み出すこと、将来の欺瞞攻撃のためユーザーの E メールを収集すること、ネットワーク・ユーザー・ネームを収集すること、及びメンバーシップ情報とネットワーク共有フォルダーのディレクトリ・リスティングをまとめることがある。
- ✧ また、オペレータは、モバイル・ユーザーのブイピーエヌ(VPN)ソフトウェアを攻撃することもある。この VPN ソフトウェアは、会社の従業員が社外から会社のネットワークにアクセスすることを許可するものである。オペレータは、VPN ソフトウェアを改ざんし、リモートのユーザー・システムを介してネットワークにアクセス・バックできるようにする。攻撃者が、正当なシステム管理者から攻撃者の存在を隠す暗号ルートキットなど、特別のネットワーク・ソフトウェアをインストールすることもある。
- ✧ これらステップの全ては、標的となった組織ネットワークへの長期に及ぶアクセスを確実に支援し、いったんネットワークに侵入した攻撃者の自由な動きを支援するものである。

また、攻撃活動のフォレンジック分析の結果は、これらの攻撃が標的にされた組織の情報セキュリティ対策を認識していることを証明している。そして、彼ら又はその代理が実施した極めて複雑な偵察活動結果を反映した活動要領の変更により、検知を避けているようである。これらの活動における攻撃者は、より能力の高いツールについては真に必要になるまで残しておき、活動環境における必要性を満たすだけに十分な洗練されたツール又は技法を利用していると思われる。

- ✧ 攻撃者は、標的ネットワーク上で最大限の「滞在」時間を確実なものとするため、標的のセキュリティ・コンフィギュレーションに対応したかなりの調整能力を持ち合わせていることを示している。これらの対応には、限定するものではないが、よりステルス性の高い通信回線への移動、別の C2 サーバーへのジャンプ、防御側の検知を察知したツールキットの迅速な削除、標的に対してのさらなる分析を支援するコンフィギュレーション・ファイルの収集などが含まれる。
- ✧ アクセスの維持に責任がある人物は、標的組織によるネットワーク防御の予期せぬ変更に柔軟に対応し得るスキルを持ち合わせていることを明らかにしている。このことは、彼らが前もってこれら不測事態への準備を行っていることを示唆するものであり、「敵の行動方針」分析と同様のものである。一般に、この準備に含まれるものとしては、冗長性のある通信回線の事前配置、複数の外部サーバー上の C2 ノード、及び標的ネットワークにおける複数の突破口がある(たいていは、標的ネットワーク中の他のコンピュータであり、既に危殆化が実施済みで待機させておき、必要時に利用する)。
- ✧ これらのオペレータが採用するマルウェアのほとんどは、様々な国々に予め確立されている指揮統制サーバーとの通信を試みる。この通信は、オペレータが犠牲システムとの交戦準備を行い、接続を確立し、制御権を奪うまでの長期間に及び継続することができる。

別の人物又はチームは、実際に標的となった情報の収集任務が付与されていると思われるが、標的ネットワークに対する優れたスキルと高度の詳細知識を持ち合わせていることを示している。彼らのネットワーク中のデータの所在確認と持ち出し活動には、一般的に冗長性、ステルス性及び詳細な準備と注意に及ぶ包括性を重視する技法が含まれている。

- ✧ これらの収集チームは、早い段階の偵察活動で収集されたと思われるネットワーク・インテリジェンスを利用して、ある場合には、サーバーとワークステーションのデータを「ステージング・ポイント(中間準備場所。staging point)」として行動する二番目のサーバーにコピーする。そして収集チームは、そのサーバー上でデータを圧縮、暗号化、分割化及び複写を行う。この活動は、標的組織から暗号化回線を介して同データを「ドロップ・ポイント(drop point)」として作動する複数の外部サーバーへの配布に先立って実施される。
- ✧ また、これらのドロップ・ポイントは不明瞭化の役割も担っており、調査者によるデータの最終あて先の確認を不可能にしている。

中国の防衛企業は、強い印象を与える速度と品質を備えた新世代の兵器プラットフォー

ムを製造している。これらの前進は様々な国内的要素によるものであるが、中国の企業スパイは､研究実施に必要な時間又は金の投資を必要としない新技術の提供源となっている。これらの収集要求事項を支援するコンピュータ・ネットワーク・エクスプロイテーションは、これまでのデータ入手に必要とされた周到な HUMINT によるアクセス方法よりも（例：合衆国市民又は同市民に接触しているエージェントと彼らのラップトップやその他の電子機器からの情報の入手)､収集可能な情報の範囲と記述の詳細さを拡大したものと思われる。合衆国における中国のスパイ活動は、合衆国カウンターインテリジェンス当局によれば、合衆国技術に対する正に最大の脅威となっており[109]、合衆国の対応を緊張させている。従来技法及びコンピュータ・ベース活動の両者によるこの違法な活動は、中国軍の近代化と新技術能力の取得に寄与しているものと判断される。

[109] 「2007 年米中経済安全保障調査委員会報告」、2007 年 11 月、7 頁、次により入手可：
http://www.uscc.gov

5　先進サイバー侵入の活動プロファイル

以下に述べる事例研究の全ては、国家の後援の下に行われたと思われる侵入とデータの持ち出し被害を受けた一つの会社を対象に、そのインシデント後の内部フォレンジック調査と情報セキュリティ専門家との討議に基づくものである。同社のインシデント内部分析の結果は、攻撃が中国経由又は中国から行われたものであることをほのめかしている。そして、侵入活動に利用された多くの技法は、中国が攻撃の発生源であると信じられている他の攻撃の活動プロファイルに一致している。本事例研究は、ただ一つのインシデントの細部事項について熟考したものである。民間セクター会社は、本事例研究が対象とする会社も含め、彼ら独自のネットワーク・アーキテクチャとリスク管理アプローチに基づき、様々な情報セキュリティ・ツールと戦略を頻繁に採用している。

合衆国のある大規模な民間会社における情報セキュリティ分析家は数年前、大量のデータが同社のネットワークから合衆国内及び海外にある複数のコンピュータに伝送されているのを検知した。そして、この活動は、他の国家後援攻撃によく関連するプロファイルに多くの面で合致していた。同分析家は、データ漏えいを停止させるため、同社のネットワークに対して速やかに障害物の設置を開始したが、既に相当量のデータが侵入者に送られてしまっていた。

この活動は数週間内に合衆国の他の大規模会社に対しても行われたが、その活動の規模は、よく訓練された指揮統制機構、具体的なデータ収集要求事項を様々な標的会社に配分する手段、及びいったん持ち出された極度に大量なデータの照合と処理能力を持ち合わせていることを示唆している。さらに、少なくともこの具体的なインシデントにおいては、攻撃者が最大の注意を払って持ち出すデータを選定したことを示している。彼らには単に「手に入れられるものは何でもいただき」そして立ち去る機会があったが、そのような策を採用しなかったこと、特定のファイルを選定し、たいていは隣接するディレクトリ・ロケーションの関連情報を無視したこと、そしてこれらの攻撃者の活動が、統制がとれた具体的な収集要求リストに基づいていると示唆していることは、一般的には高度に専門家された作戦に見出される特性である。

攻撃者は、下記に述べるインシデント間、ファイルを開き内容をレビューすることはなった（もっともそれには許可が求められていたが)。その代り、彼らが欲するファイル又はフォルダーに直ちに進み、それらを持ち出すためのステップを開始した。このことは、彼らがディレクトリ・コンテンツをオフラインでレビューしていること、及び彼らが、持ち出し可能なファイル・ディレクトリ・リスティングを含め、この会社に対する詳細な偵察

活動を実施するためのネットワーク・アクセス権を既に取得していたことを示唆するものである。

これらの活動技法の種類は、アマチュア・ハッカーが地域的に広く分散して活動する特性を示すものではない。個々のオペレータの所属を確立するのは不可能であるが、この活動の企画に必要な調整は、仮に彼らが直接国家又は軍組織に所属してないフリーランスであったとしても、彼らが本格的な優れた組織と統制力及び具体的な収集目的を持っていることを示唆するものである。このことは、彼らが、容易にアクセスが可能なデータをできるだけ沢山収集するのではなく、目的とするデータだけを収集した証拠によって裏付けられる。本事例において盗まれたデータの種類と特殊性は、エンドユーザーが既に明らかにされており、かつ、彼らは盗まれたデータを利用するに当たって科学技術資源を自由に使用できる立場にあることを示唆している。

情報セキュリティ調査の実施に当たって、オペレータの属性を明らかにすることは最も困難な部門であるが、個人やグループもどきのハッカーは首尾一貫した方法で活動する傾向がある。具体的には、好みとする特定のツールを誇示したり、ユニークなキーボード操作を示したり[110]、時には複数の標的全般にわたって、同一種類のデータを攻撃目標とする傾向にある。本事例からオペレータに対する確固とした属性データを入手できなかったものの、本事例は中国による合衆国ネットワーク侵入に属すると判断された他のインシデントに一致している。

侵入者達は、複数日に及ぶ本事例インシデントの間、複雑なデータ持ち出し活動を行った。そして、このインシデントに関連する活動そのものは比較的短い期間に行われたが、この活動支援に必要な準備と偵察は数ヶ月にわたり継続して実施されたと思われる。この活動を実施したチーム又は複数の人物が、統制に従った行動と標的としたネットワーク・アーキテクチャに対する深い知識を示したことは、これらのオペレータが標的ネットワークに係る詳細な全体像を、根気よく数ヶ月にわたって収集したと思われることを示唆するものである。

- ✧ 同様のリモート通信と管理ツール及び活動技法が、本インシデントと他の会社のインシデントの初期段階で利用された。彼らはときどき、中華人民共和国に設けられた IP アドレスを持つホストと会社の内部ネットワーク上のサーバー間の通信回線を利用して活動した。このときに観察された技法は、他の民間会社への同様の侵

110 コンピュータ・ネットワーク侵入の流れにおける個人の「キーボード上の振る舞い」は、ハッカーが何度もある役割を果たす上で明らかにするに違いない特定の習慣を示すことになる。巧緻性、頻度、コマンドの組み合わせ、及びキーボード・エントリー間の経過時間は、個々の攻撃者の「フォレンジック・プロファイル」作成の助けとなり得るものである。

入の際に利用された技法と一致した。

- ✧　この活動の分析結果からは、敵対者は予め具体的なディレクトリ、ファイル・シェア[111]、サーバー、ユーザー･アカウント、従業員の氏名、パスワード・ポリシー及びネットワーク上のグループ・メンバーシップを、おそらくは彼らによる詳細な偵察フェーズの間に明らかにしていたことを示唆している。
- ✧　彼らは、ファイルを持ち出す前に、いかなるファイルも内容をレビューするために開くことはしなかった。このことは、彼らが事前に内容を知っていたか、又は少なくとも彼らがデータを盗むに当たって、データのファイルネームを指定されていただけであったことを示唆するものである。

敵対者は、侵入活動において少なくとも 2 つのグループを利用した。それらは、突破チーム（会社の情報セキュリティ分析家は「第一チーム」と分類した）と標的とされたデータの収集と持ち出し責任がある収集チーム（同じく「第二チーム」と分類した）である。

- ✧　各チームは、別個のツールキットを採用し、それらを独特の方法で利用した。このことは、各チームの活動目標が異なるだけでなく、キーボードには異なる人物が配置されていたことを示唆するものである。
- ✧　両チームは、会社のネットワークに設置されたホストに活動基地を維持した。これは、彼らの長期間に及ぶ密かな通信を支援するため、外部の場所で必要に応じ利用する場合に備えたものである。

会社の情報セキュリティ分析家は、このデータの持ち出しに先立ち、この種タイプの洗練された攻撃者に起因すると考えられる活動を検知したが、危殆化されたホストからのトラフィック量が概して少ないとみなされたことから、主にアクセスの維持と滞在が活動の中心のように思った。会社の情報セキュリティ・スタッフは、最終のデータ持ち出しに先立つ数ヶ月もの間、これらの危殆化の検知と阻止活動を実施した。それにもかかわらず、攻撃者の活動は、単に新たなエントリ・ベクターを作ったか、又は別の前もって確立された会社ネットワーク・アクセス方法に戻ったように見えるだけであった。ネットワークの正確なマップを編集するための偵察フェーズは、その間を通じて極めて組織的かつ静的であるかのように思えた。敵対者は、サーバー、ファイル・シェア、個々の従業員、ユーザー・グループ、及び後で複雑なデータの持ち出し支援に必要な証明書を明らかにした。

図 7 は、敵対者が合衆国商用ネットワークに侵入し、データ持ち出し活動を行った際のダイアグラムである。この活動は洗練されたものであり、おそらくは国家が後援しているものと考えられる

[111] File sharing：ネットワークを利用して、複数のコンピュータで一つのファイルを利用すること。

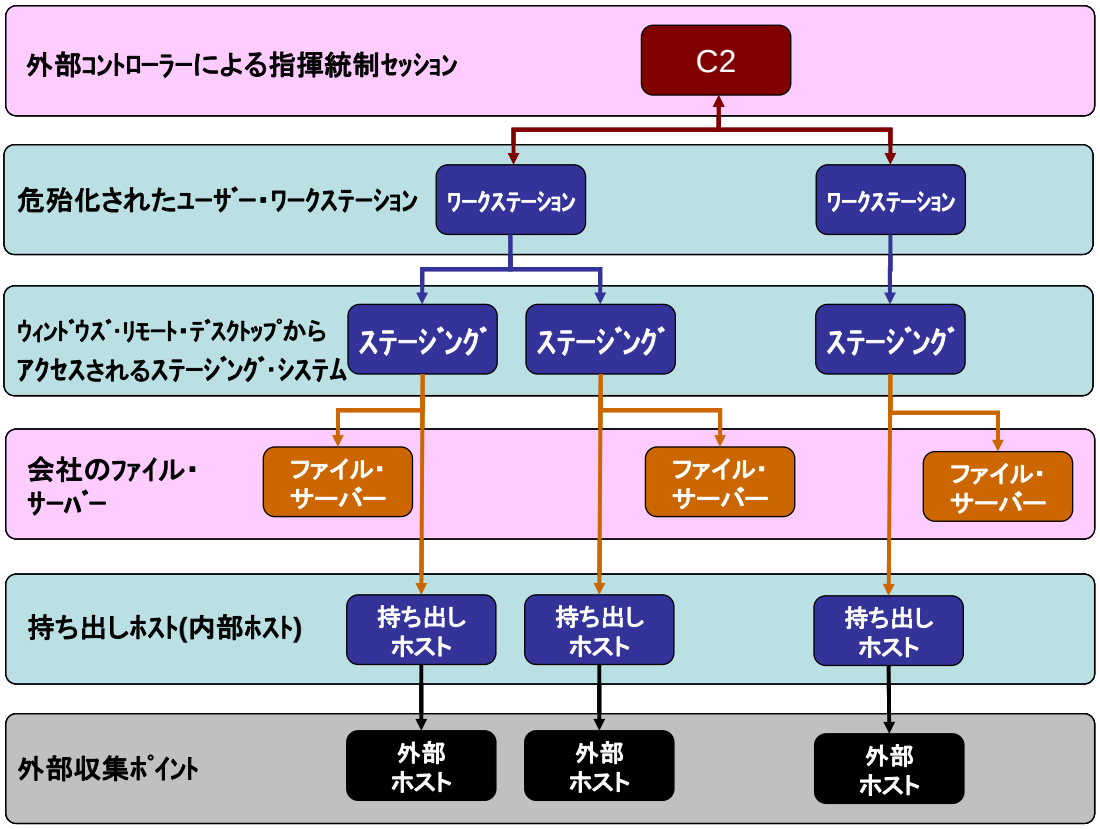


図 7：データ持ち出し活動ダイアグラム

5.1　侵入者の指揮統制インフラ

侵入者によるデータの持ち出し前と持ち出し中における活動の分析結果は、彼らの指揮統制アーキテクチャーが予め盗まれた正当なユーザー・アカウントに依存していることをほのめかしている。このアカウントは、会社の内部サーバーへのアクセスを認可するものである。彼らは、いったん認可されると、予め危殆化した会社ネットワーク内の様々なコンピュータとの通信を確立した。そしてオペレータは、彼らの既存通信回線内のリモート・デスクトップ・プロトコル(Remote Desktop Protocol: RDP)[112]を、道を掘るようにして進み、基本的なアクセスの維持から最終的なデータ持ち出し制御に及ぶ活動を行うため、標的にされたホストとの接触を確立した。盗まれたその他のアカウント・ネームとパスワードは、コンピュータ、ネットワーク・シェア、フォルダー、ファイルなどの保護された資源にアクセスするため、必要に応じ利用された。

112　ターミナル・サービスを稼動しているコンピュータにユーザーが接続することを許可する多重チャネル・プロトコルをいう。

- ✧　プロキシ・ログとフォレンジック･データの分析結果は、オペレータがデータの持ち出しに至る数日の間に、約 150 回にも及ぶネットワーク・アクセスに数十の従業員アカウントを利用したことを明らかにしている。
- ✧　彼らは、大きな権限を持つ管理者用アカウントをときどき利用し、パスワードの代わりに NTLM ハッシュ[113]を直接プロキシ認可メカニズムに伝送した[114]。危殆化されたドメイン・コントローラーから直接獲得したパスワード・ハッシュの利用は、ブルートフォース・パスワード・クラッキング・ツールに対する防衛用に設置されていた全ての 2 要素認証（Two-Factor Authentication: T-FA）技法に打ち勝つためと思われる。
- ✧　ドメイン・コントローラーからパスワード収集ツールを利用して獲得した NTLM ハッシュの利用は、ブルーフォース・パスワード・クラッキング・ツールに対する防衛のため設置されていたすべてのマルチファクター認可技法に打ち勝つためと思われる。
- ✧　また、敵対者は、組織の主ドメイン内にあるグループ・メンバーシップ・アカウントを繰り返し一つ一つ列挙した。これは、敵対者が特定のユーザーに制限されているファイルをアクセスする際に、利用できる従業員のアカウントを明らかにするためである。

5.2　標的データの中間「ステージング・サーバー」への移動

敵対者は、このインシデントにおける最初の数日間で、持ち出し用に選定したデータを会社のファイル・サーバー（通常はここに保管されている）から、中間ステージング・ポイントとして活動するマイクロソフト･エクスチェンジ E メール･サーバーに移動した（図 7 を参照。この図において、移動はステージング・システムと会社のファイル・サーバー間で行われる）。敵対者によるネットワークの偵察により、彼らは最も高い性能とネットワーク・スループットを提供するサーバーを選ぶことができる。繰り返し強調するが、敵対者のこれらサーバーの識別と選定能力は、この持ち出し活動に先立って行われた会社のネットワークに対する詳細な偵察によって得られた正確な知識によるものである。

攻撃者は、明確な指揮統制方針を確立の上、活動におけるステージングと持ち出しフェーズに利用する適切なホストを識別することにより、ファイル・サーバーからステージング・ポイントへのデータ移動の準備を開始した。入手できたデータに基づく分析結果は、

---

113 NTLM ハッシュ：Windows NT LAN Manager(NTLM)認証に利用されるパスワード・ハッシュをいう。

114 多くのプロキシ・サーバーは、Internet/WWW/FTP アクセスなど、保護された資源へのアクセスが許可される前に、NTLM チャレンジ/レスポンス認可を求めるよう構成できる。攻撃者が認可ハッシュを所有していれば、最初にパスワードを「解読(crack)」してから認可サービスを受けるために再ハッシュする代わりに、攻撃者はそのハッシュを直接利用することができる。

敵対者が標準のウィンドウズ・ファイル・トランスファー・ツールを利用して、標的とされたデータをシェアからステージング・サーバー[115]へ移動したことを示している。

- ✧ 収集チーム(第二チーム)メンバーと思われるオペレータは、内部ホストを C2 ノードとして利用し、暗号化された RDP セッションを介して様々な内部 E メール・サーバーに対する複数の接続を、これらのマシンにデータをステージングする前に確立した。
- ✧ フォレンジック・データは、ステージング活動が行われる数日前に、C2 ノードとして利用した内部ホストと E メール・サーバー間において短期の通信が増加しているのを明らかにした。このプロセスは、以降の活動の全フェーズにおいて利用される資源の識別と確認を行ったものであると思われる。
- ✧ また、敵対者はこの活動と同時に、持ち出し活動に利用する E メール・サーバーとおそらくは彼らの管理下にある思われる外部のウェブサイトとの間の通信回線を確立した。攻撃者は活動を準備する際に、この回線を主 C2 チャネルとして利用し、少なくとも内部 E メール・サーバーの 7 つを制御した（図 7 の外部収集ポイントを参照)。

オペレータは、データをステージング・サーバーに移動した後、標的にされたファイルネームを漠然としたラベルに変更した。これは正当なウィンドウズ・アプリケーションに似せたものであり、ステージング・サーバー上では害がないと見せかけるために選定されたと思われる。

- ✧ 攻撃者は、いったんステージング・サーバーへのデータ転送を完了すると、ファイル暗号化と圧縮を行い、多量の RAR アーカイブ[116]に変換した。これは持ち出しの準備のためであり、すべてが正確に同一サイズで配分された[117]。
- ✧ 会社内の情報セキュリティ分析家は、このプロセスに利用されたツールと技法が、会社のネットワーク上で以前検知した活動に利用されたものと近似していると言及した。このことは、この活動が同じ実体によるものであったか、さもなければ他の侵入活動に責任があるオペレータが、彼らの標的若しくは活動についてデータの共有手段を持っていたか、そのいずれかであったことを立証するものである。

---

115 ステージング・サーバー：本番環境へとアプリケーションが展開される直前に、本番と同様のテストを行うサーバーをいう。

116 RAR アーカイブ：RAR 形式のデータ圧縮ファイルをいう。

117 注解：RAR アーカイブスのサイズは、すべて正確に 650 メガバイトであった。これは標準的な CD ROM の最大容量であり、将来における保管又は伝達媒体に適したものであることを示している。

5.3　内部ネットワークからのデータの持ち出し

彼らは、彼らの組織的な準備をつらつら考えると、会社のネットワークからデータを移動させるため、ほとんど縦一列状態の 7 つのサーバーを利用していた。このことは、このフェーズの活動における最優先事項が速度であったことを示唆している。内部ネットワークから外部へのデータの移動は、全活動における最もぜい弱なフェーズといえる。なぜなら、会社がネットワーク境界に防御ツールを設置していること、及びこの活動の準備としてネットワーク中に数日間存在する間に会社から検知される唯一のポイントだからである。

持ち出し活動の最終段階は、標的とされたすべてのデータが中間ホスト上に展開された夕方（この会社の現地時間）に開始された。オペレータは、データの持ち出しに先立ち、次に示す準備に特段の注意を払った。それらは、全体を統制する C2 チャンネルを確立すること､彼らの接続を確認すること､(可能性として)彼らの手順のリハーサルを行うこと、及び実際の持ち出し開始前に利用可能なバンド幅のチェックを行うことであった。

- ✧　オペレータは、単一 E メール・サーバーからの持ち出しが開始された後、標的とされた領域におけるすべての E メール・サーバーを一つ一つ列挙した。このことは極めて重要なことである。なぜなら、彼らが利用したリクエストは、サーバーが設置されている地域におけるこれらサーバーに対する会社内部標準ネーミング慣行であったからである。それらの知識は、当該ネットワークに対する極めて詳細な偵察によってだけ得られたものである[118]。コマンドは、数十にも及ぶサーバーのリストを報告した。彼らがステージング又は持ち出しポイントとしてのいずれかの活動に利用したのは、そのうちの 75%であった。
- ✧　この活動に参画したチームは、内部サーバーから大きなビデオ・ファイル(20MB)をアクセスするため、会社外へのデータ移動用に利用する各サーバーを指定し、実際の持ち出しの準備をした。攻撃者は、それぞれの場合において、そのビデオのわずかな部分を受信しただけでその接続を終了させた。この切り詰められたダウンローディングは､攻撃者が当該ファイル自身の内容を見るつもりではなく､大容量のデータ伝送に利用できるバンド幅をテストしていたと思われる。

攻撃者は、正当なユーザー・アカウントを利用して活動し、会社のデスクトップ・マシンの一つを制御した。そして、このマシンを C2 ノードとして利用し、すべての持ち出し活動に係る複数のサーバーへの指令を行った(会社の分析家は、C2 ノードとして総計 4 台

---

[118] 組織のネットワークが広大な地域に分散している場合、たいていそれらのサーバーに対するネーミング慣行を利用する。それらは、サーバーの物理的設置場所、次に会社内部組織の細目又はサーバーの役割を示すコードなどであり、例として XY 地区のモンタナに設置されているプリント・サーバーの場合は、内部的に「MTXYP012」と名づけられる。本事例では、攻撃者は彼らの標的行為に利用した慣行を正確に知っており、彼らが標的にしたデータが所在する地域のすべてのサーバーを調査した。

のデスクトップ・マシンが利用されたことを明らかにした)。この特殊な C2 ノードは、ステージング・サーバー1 台、その他 2 台の既知中間ホスト含む複数の内部サーバー、及び合衆国に所在する外部 IP アドレス 1 個に接続されていた。

- ✧ 内部 C2 ホストの一つは、合衆国に本拠地を置く商用インターネット・サービス・プロバイダーの DSL[119]顧客との接続を確立した。このプロキシ接続は、すべてのデータの持ち出しフェーズの間、オープン状態を維持した。このノードはその間、RDP を介して、少なくとも 8 つの外部ホストと接続した。そのうちの一つは香港に所在するものであった。[120]
- ✧ 本インシデントにおけるトラフィック・フローの分析結果は、攻撃者が大量のデータを、ステージング・サーバーから会社のネットワーク外の持ち出し転送ポイントとして利用したサーバーに移動したことを示している(「持ち出しホスト」と「外部収集ポイント」間の接続については、図 7 を参照)。

情報セキュリティ防衛を突破する責任を持つ第一チームのオペレータは、実際のデータ持ち出し開始に先立ち、当たり障りのないファイルを利用して彼らの担当部分のリハーサルを実施したと思われ、そのときに 3 つの RAR アーカイブ・ファイルを別個の FTP セッションを介した伝送を試みた。

オペレータのコマンド・チャネル活動の分析結果は、この会社のネットワークから持ち出されたデータを受信するとしていた 2 つの外部ホストについて、彼らが重大な問題に遭遇したことを示している。また、彼らはカスタムの FTP クライアントとサーバー・ソフトウェアを試みたが、理由不明で失敗に終わった。そのオペレータは、これらのサーバーとカスタム FTP ソフトウェアの一つを見捨てた。これは、ゆっくりとした信じられないほどのデータ伝送率によるものと思われる。そして、データ持ち出しの残余の部分に対しては、標準の FTP サーバー・ソフトウェアを 5 つ以上の信頼性のあるリモート・ホスト上で走らせた。

- ✧ オペレータはこの持ち出し活動の最終日、それまで彼らが毎日開始していたのと同じ夕刻に、FTP 接続を内部持ち出しサーバーの一つと外部ホストの間に確立した。彼らは、大きなファイルが後続するゼロ・バイトのファイルをアップロードすることにより、同接続が適切に働くことを確認した。オペレータは、この接続が適切に機能することにどうやら満足し、この内部サーバーをログアウトし

119 DSL：Digital Subscriber Line。デジタル加入者線をいう。
120 香港との接続は、不首尾に終わった。これは、データを受け取るための注意深いステップが合衆国に配置されたサーバーに対して実施されてことを考慮すると、偶発事故と思われる。

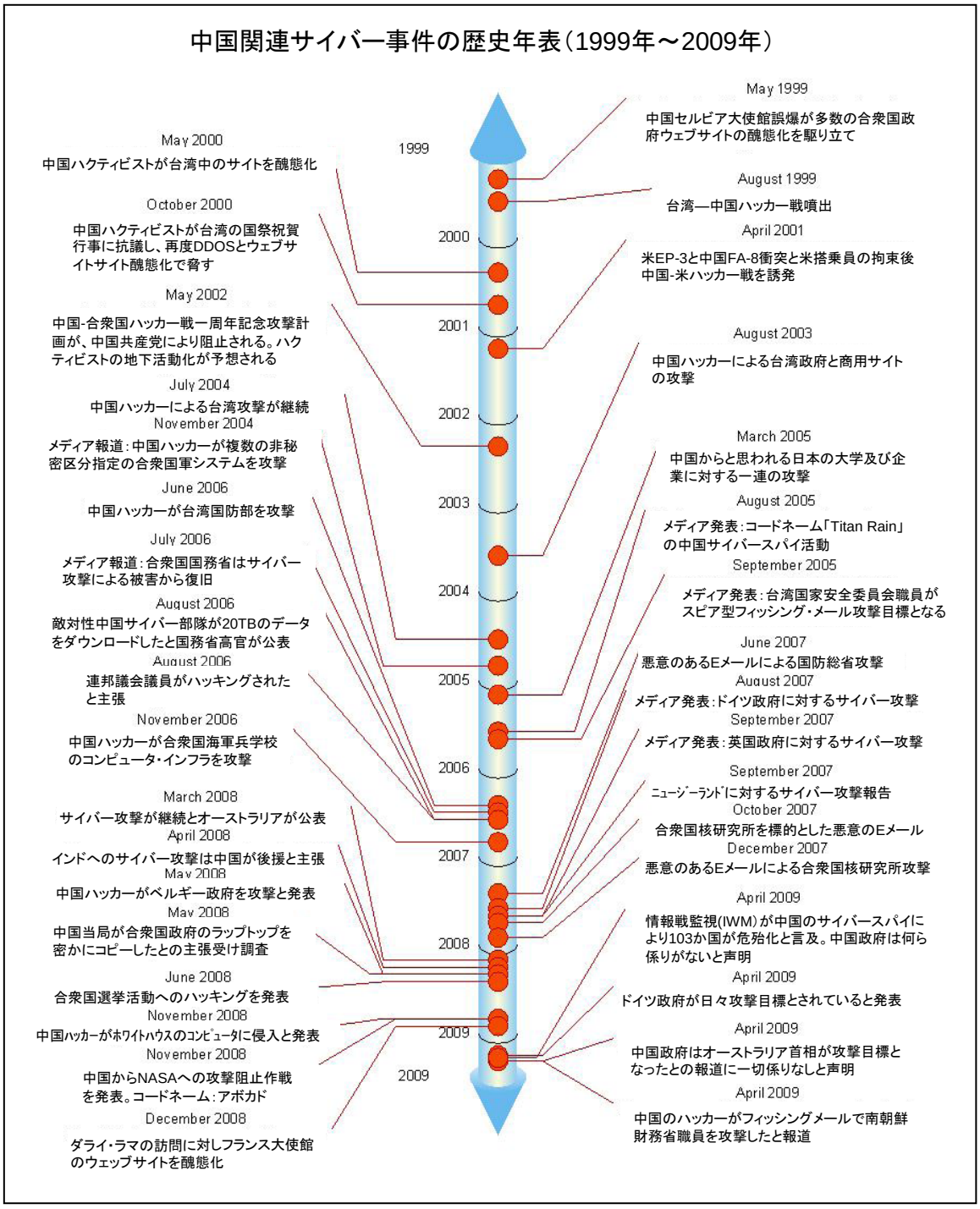
た。

- ✧　オペレータは、30 分以内にこの同じ内部サーバーに再接続した。そして、同じ証明書を利用し、会社の企業機密データを含む最初の暗号化された RAR ファイルの移動を試みた。彼らは 2 分後、他のファイルの移動を試み、そしてログアウトした。彼らは数分後、再接続し、第三のファイルの移動を試みた。各場合において、FTP 接続は理由不明のまま早期に終結した。このことは、このチャネルを介して小さなファイルの伝送は首尾よく行われたが、大きなファイルの場合は失敗の原因となったようである。
- ✧　そこで彼らは、暗号階層が上乗せされたカスタム FTP ソフトウェアを利用する新たなリモート FTP サーバーに伝送することを試みた。攻撃者の FTP ソフトウェアは、カスタム・コマンド「SORT」を実行した。これは、クライアントによって出され、サーバーに通常の平文のファイル伝送に替えて暗号通信を受け取るシグナルとして認識させるものであった。そして、この同じソフトウェアを新たなリモート・ホスト上でほとんど直ちに試みた。そして再度、テスト伝送に失敗した。彼らは、最後のテストにおいて、最初のリモート・サーバーに接続を戻した。このサーバーは、彼らのカスタム FTP サーバー・ソフトウェアを走らせているものであり、伝送を試みるものの、またもや失敗した。
- ✧　そして彼らは、第二の合衆国大学に接続し、変更が行われていない FTP サーバー・ソフトウェアを利用することにより、手動で大きな RAR ファイルの移動に成功した。オペレータはこの直後に、5 つのリモート・ホストに対して一連の自動化された、冗長性のある伝送を確立した。この主たるデータの持ち出し活動の成功率を最大化するため、5 つのサーバー上にこの同じサーバー・ソフトウェアが動いていた。

情報セキュリティ・スタッフは最終的に、データ持ち出しの中途段階で検知し、遮断したが、相当量の会社データがネットワークを離れた後であった。そこで、会社のネットワーク上の侵入防護システムは、さらなる活動を警告しブロックするよう調整された。そして次の 5 時間は、オペレータによる伝送試みを検知し続けた。このことは、彼らが計画通りの持ち出しを完了する前に妨害されたことを示唆するものである。この会社の情報セキュリティ分析家は、この持ち出し活動が意図した総データ量を決定する手段を持っていなかった。

6　重大な中国関連サイバー事件の歴史年表(1999 年～2009 年)

下図は、1999 年～2009 年までの中国が関連したと思われるサイバー事件の歴史年表である。これらの事件の細部は、次節に記述してある。



7　中国のコンピュータ・ネットワーク・エクスプロイテーション事件年代記

中国が、合衆国及び外国のネットワークを対象に実施したとされるコンピュータ・ネットワーク・エクスプロイテーション事件の年代記は、次のとおりである。

1999

1999 年 5 月：1999 年 5 月の中国セルビア大使館に対する合衆国誤爆事件は、中国ハッカー・コミュニティからの激しい攻撃を駆り立てた。そして、合衆国政府ウェブサイトの醜態化が中国ハッカーによって行われた[121]。

1999 年 8 月：当時の台湾総督 Lee Teng-huit による人民共和国との「国家対国家」ベースが好ましいとした発言に対し、「台湾―中国ハッカー戦」が噴出した。中国のハッカーは、無数の台湾の政府、大学及び商用サイトを醜態化した。これに対して台湾ハッカーが反撃し、中国政府のウェブサイトを親台派言語で醜態化した[122]。

2000

2000 年 5 月：中国ハッカーが、Chen Shui-bien の宣誓就任を抗議して、台湾政府のウェブサイトを反台湾政治声明で醜態化した[123]。

2000 年 10 月：中国ハッカーが、台湾の国祭日祝賀行事に抗議して、台湾政府と民間のウェブサイトに対しサービス妨害攻撃と醜態化を行うと脅迫した[124]。

2001

2001 年 4 月：合衆国海軍 EP-3 偵察機と人民解放軍海軍(People's Liberation Army Navy: PLAN)F-8 戦闘機の衝突、及びそれに引き続く海南島での Ep-3 搭乗員の 11 日間の拘留が、最初の「中国―合衆国ハッカー戦」を誘発し、米中両サイドからサービス妨害攻撃とウェブ醜態化が政府と民間サイトに対して行われた[125]。

2002

2002 年 5 月：中国民間人ハッカーが、最初の中国―合衆国ハッカー戦の 1 周年記念日を祝うため、合衆国ウェブサイトに対する大規模攻撃計画立案を開始した。彼らの攻撃計

---

121 Ellen Messmer 著、「コソボ・サイバー戦激化：政府によれば中国ハッカーが合衆国サイトを攻撃目標にしたとされる」、CNN.com、1999 年 5 月。

122 Fred Jame 著、「ウェブ・ハッキング『戦』における中国と台湾」、MacWeek.com、1999 年 8 月。

123 「中国の台湾ウェブサイト・ハッキング計画」、The Straits Times、2000 年 10 月。

124 上記同書。

125 Tang と Rose 共著、「中国が大量ハッキング攻撃を警告」、CNN、2001 年 5 月。

画は、中国共産党が発布した外国のネットワークに対する愛国的ハッキング行為に係る厳しい語句での譴責文書により、終わらせられた[126]。

2003

2003 年 8 月：中国本土湖北省と福建省のサイトで活動しているハッカーが、30 の台湾政府機関と少なくともその 2 倍に及ぶ台湾の会社に侵入した。その攻撃活動の中心は、国防部、選挙委員会及び国家警察本部が主であった。これは、台湾政府と民間企業に対する一連の継続した攻撃の一部であって、2004 年の台湾の財務部や国民党などの著名なウェブサイト攻撃まで続いた[127]。

2004

2004 年 6 月～7 月：台湾に対する攻撃は、2004 年の台湾の財務部、国民党、民主進歩党(Democratic Progressive Party: DPP)及び国防部(Ministry of National Defense: MDD)軍事報道庁に対する標的行為に至るまで継続した[128]。

2004 年 11 月：合衆国メディアは、次のように報告した。中国のハッカーが、アリゾナ州 Huachuca 陸軍駐屯地にある合衆国陸軍情報システム・エンジニアリング司令部、アーリントンにある国防情報システム庁、カリフォルニア州サンディエゴにある海軍海洋システム・センター及びアラバマ州にある合衆国陸軍宇宙戦略防衛施設に及ぶ複数の非秘密区分指定合衆国軍システムを攻撃した[129]。

2005

2005 年 5 月：中国及び南朝鮮から発せられたと思われる一連の攻撃が、非常に多くの日本の大学と企業のウェブサイトに対して行われた。この攻撃をもたらしたのは、日本の文部科学省が日本の第二次世界大戦中の行為に係る主要な歴史的事実を削除したとされること、及び日本の国連安全保障会議常任理事国加入の企てに対する中国の反対姿勢によるものとされている[130]。

2005 年 8 月：メディアが、その表紙にコード・ネームが「タイタン・レイン(Titan Rain)」とされた中国コンピュータ・ネットワーク・エクスプロイテーション活動記事を掲載し、

---

126 Pamela Hess 著、「中国は合衆国に対するサイバー攻撃の繰り返しを阻止」、UPI、2002 年 10 月 29 日。

127 Wendell Minnick 著、「増大するサイバー猛攻撃に直面する台湾」、Army Times Publishing、2006 年 6 月。

128 上記同書。

129 Tom Espiner 著、「中国人ハッカーが合衆国防衛軍を攻撃」、Silicon.com、2005 年 11 月。

130 Anthony Faiola 著、「サイバー戦：中国対日本」、NSNBC News、2005 年 5 月。

国防総省システムに 2003 年来侵入を行ったと報道した[131]。

2005 年 9 月：台湾のメディアによれば、台湾の国家安全委員会が悪意のある添付資料を含む社会的に工作された E メールを介して、攻撃目標にされたと報道した。この添付資料を開けると、受取人のホストが感染し、侵入者が検知されずに戻れるバックドアをインストールしたとされている。この E メールの件名には「兵器調達」と「自由」の語句が含まれていた[132]。

2006

2006 年 6 月：台湾のメディアは、中国のハッカーが台湾国防部(Ministry of National Defense: MND)と台湾米国協会(American Institute in Taiwan: AIT)を攻撃したと報じた。同攻撃者は、社会的に工作された E メールを用いて攻撃を行い、MND について外見上誹謗運動とみられる誤情報の流布を企てたとされている。また、同攻撃者は、MND の電気通信プロバイダーである Chunghwa テレコムのウェブ・メール・システムから、アカウント・ログイン証明書を盗んだ[133]。

2006 年 7 月：合衆国のメディアは、侵入者が合衆国国務省(Department of State: DoS)のネットワークに侵入し、機微情報とユーザー・ログイン・証明書を盗むとともに、攻撃者がいつでもシステムに戻れるよう、多くのコンピュータにバックドアをインストールしたと報じた。DoS のシステム管理者は、調査が完了するまでインターネット・アクセスを制限せざるを得なかった。中国の参加については明らかにされていないが、中国、北朝鮮及び日本との外交政策調整任務が付与されている東アジア・太平洋局における問題は極めて重大であったと報じた[134]。

2006 年 8 月：国防総省の高官は、中国内で活動している敵対性民間人サイバー部隊が NIPRNET に対し攻撃を行い、20 テラバイトにも及ぶデータをダウンロードしたと公表した[135]。

2006 年 8 月：中国の人権侵害歴について忌憚のない意見を述べる酷評家として有名な

---

131 Bradley Graham 著、「ハッカーが中国のウェブサイトを介して攻撃」、The Washington Post、2005 年 8 月。

132 「国家安全委員会のコンピュータがハッカーの E メール攻撃の標的にされた」、Liberty Times、2005 年 9 月。

133 Wendell Minnick 著、「増大するサイバー猛攻撃に直面する台湾」、Army Times Publishing、2006 年 6 月。

134 「国務省において大規模ハッキングが発見された」、Buzzle Staff and Agencies、2006 年 7 月。

135 Dawn Onley、Dawn and Patience Wait 共著、「赤い嵐が吹き始める：中国から始まる国家サイバー攻撃阻止のための国防総省の活動」、Government Computer News、2006 年 8 月。

連邦議会議員が、中国人ハッカーが彼のオフィスの彼と彼のスタッフのコンピュータに侵入したと主張した[136]。

2006 年 11 月：中国のハッカーが合衆国海軍兵学校のコンピュータ・インフラを攻撃した。おそらく、ネットワーク上のウォーゲーム情報を攻撃目標にしたものと思われる。同校のウェブと E メール・システムは、調査実施の間の少なくとも 2 週間利用できなかった[137]。

2007

2007 年 6 月：メディアが、国防総省内部部局(Office of the Secretary of Defense: OSD)の E メール・システムが侵入され、約 1,500 のコンピュータがオフラインとなったと報道した。

2007 年 8 月/9 月：ドイツのメディアが、ベルリン当局は PLA とつながる中国ハッカーがマイクロソフト・ワードとパワーポイント文書を利用している様々なシステムにバックドアをインストールしたと確信している、と報道した。攻撃目標にされたドイツ政府組織には、首相官邸、経済技術省及び教育省が含まれる。ドイツ政府当局は、サイバー攻撃の 60%は中国から発生したものと推察している。その多くは、蘭州、広東及び北京の都市からであるとしている[138]。

2007 年 9 月：連合王国のメディアは、中国人ハッカーが連合王国の外務省を含む政府省庁を攻撃したと報じた。当局によれば、それほど大きな影響を被るには至らなかったとされている。もっとも、休みなく続く中国サイバー攻撃活動は、絶え間のない問題であると認識されている[139]。

2007 年 9 月：ニュージーランド諜報部は、最近のサイバー攻撃に中国政府が関与していると示唆した。中国政府は、いかなる関与も否定した。この件については、合衆国同盟国に対する攻撃に関しても同様の報告がなされている[140]。

2007 年 10 月：合衆国のメディアは、中国がオークリッジにあるオークリッジ国立研究所の 1,100 人の従業員を攻撃目標に、少なくとも 7 つのバージョンの社会的に工作された

136 Steven Schwankert 著、「合衆国議員が彼らのコンピュータにハックしたとして中国を非難」、IDGNS、2008 年 6 月。
137 上記同書。
138 Ulf Gartzke 著、「ベルリンは中国のサイバー攻撃に憤慨」、The Weekly Standard、2007 年 8 月。
139 Richard Norton-Taylor 著、「タイタン・レイン：中国人ハッカーは如何にしてロンドン官庁街を攻撃目標としたか」、The Guardian、2007 年 9 月。
140 Liam Tung 著、「中国はニュージーランドのサイバー攻撃を非難」、CNET News、2007 年 9 月。

E メールを送りつけた疑いがあると報告した。7 人のスタッフが悪意のある添付資料を開けた結果、攻撃者に機微データのアクセスと窃盗を許すことになった可能性がある。この機微データには、核兵器研究所のデータベースに記憶されている 1990 年からの居住者記録が含まれている[141]。

2007 年 12 月：英国の国内インテリジェンス機関 MI5 は、300 の最高経営責任者、会計専門家、法定会社及び警備組織に警報を出し、中国国家組織が後援するサイバー攻撃と電子スパイ行為について警告した。この警告には、人民解放軍(PLA)が中国におけるビジネス活動を攻撃目標としていること、及びインターネットを利用して企業機密情報を盗み出すことが含まれている。[142]

2008

2008 年 3 月：オーストリアの保安機関が、継続したサイバー攻撃の犠牲となっていることを認めた。しかし、中国を非難するまでには至らなかった。[143]

2008 年 4 月：インド政府の高官が、中国は「インド政府とインド民間セクターのネットワークに対する攻撃のほとんど」を後押ししていると主張した。[144]

2008 年 5 月：ベルギー政府は、政府のシステムが中国を本拠地として活動しているハッカーによって複数回にわたって攻撃目標にされたと発表した。[145]

2008 年 5 月：合衆国政府当局は、当時の商務省長官 Carlos Gutierrez'が中国を訪問した際に、中国当局が合衆国政府のラップトップの内容を密かにコピーしたとする主張を受け、調査した。[146]

2008 年 11 月：メディアは、中国のハッカーがホワイト・ハウスの情報システムに幾度となく侵入したと発表した。この侵入は、システムにパッチングを行う前の短期間に行われたとされている。[147]

---

141 「中国はオークリッジ国立研究所へのハッキングを企てたと思われる」、Homeland Security News、2007 年 12 月。

142 Rhys Blakely、Jonathan Richard、James Rossiter 及び Richard Beeston 共著、「中国のサイバースペース・スパイ脅威に対する MI5 の警告」、The Times、2007 年 2 月。

143 Rose Peake 著、「オーストラリアはサイバー攻撃を確認」、Canberra、2008 年 3 月。

144 Dan Goodin 著、「インドとベルギーは中国のサイバー攻撃を公然と非難」、The Register、2008 年 5 月。

145 上記同書。

146 Steven Schwankert 著、「合衆国議員が彼らのコンピュータにハックしたとして中国を非難」、IDGNS、2008 年 6 月。

147 上記同書。

2008 年 11 月：雑誌 Business Week は、過去数年間にわたって、ケネディ宇宙センターとゴダード宇宙飛行センターを含む NASA の最も重要なサイトのいくつかが、重大なサイバー侵入を受けたと発表した。中国からの攻撃を阻止する作戦のコード・ネームは「アボカド(Avocado)」であった。攻撃には、NASA のトップ職員に対する社会的に工作された E メールがふくまれていた。盗まれたデータの中には、性能とエンジン・データを含む宇宙シャトルの運用に係る詳細事項が含まれていた。[148]

2008 年 12 月：hack4.com メンバーの中国人ハッカーは、フランス大統領がダライ・ラマをちょっと訪ねた後に、政治的な動機付けに基づき合衆国、連邦王国、中国及びカナダにあるフランス大使館のウェブの醜態化を行った。[149]

2009

2009 年 3 月：カナダの調査チームが、世界中の 1,300 以上にも及ぶホストを攻撃した GhostNet サイバー・スパイに係る研究成果を公表した。これらのホストには、世界中のドイツ、インド、パキスタン及びポルトガル大使館、並びにインドにあるチベット亡命政府が含まれている。カナダに本拠地を置く情報戦監視(Information Warfare Monitor: IWM)は、130 か国にも及ぶ非常に多くの政府と民間の情報処理システムが危殆化されたと言及している。このネットワーク攻撃のすべては、中国の海南島から行われた。中国政府は、これらについての責任又は国家が後援したとするすべての非難について、一切係わりがないと言った。[150]

2009 年 3 月：Philippine Daily Inquire は、GhostNet 研究成果を引用し、中国に本拠地を置くサイバー・スパイによってフィリピン外務省(Department of Foreign Affairs: DFA)のコンピュータ・ネットワークがハックされたと公表した。[151]

2009 年 4 月：メディアは、ドイツ政府が政府ネットワークに対して日々攻撃が行われていることを示した、と発表した。メディアは、ドイツ外務省が激しい攻撃目標となっていることに言及するとともに、社会的に工作された E メールによって侵入されていると報

---

148 Keith Epstein 及び Ben Elgin 共著、「ネットワーク・セキュリティ突破が NASA を悩ませる」、Business Week、2008 年 11 月。

149 Asian News International、「中国にあるフランス大使館ウェブサイトがハックされた」、HT Media Limited、2008 年 12 月。

150 John Markoff 著、「巨大スパイ・システムが 103 か国のコンピュータから不正収得」、New York Times、2009 年 3 月 28 日。

151 Aning、Jerome and Olchondra 及び Riza T 共著、「フィリピン共和国政府ウェブサイトはハッキングにぜい弱」、Philippine Daily Inquirer、2009 年 3 月。

じた。[152]

2009 年 4 月：オーストラリアのメディアは、中国のサイバー・スパイが E メールと携帯電話を介してオーストラリア首相を攻撃目標にしていると報じた。中国政府は、これら非難について一切係わりがないと言った。[153]

2009 年 4 月：メディアは、中国に本拠地を置くハッカーが南朝鮮財務省のイントラネットに侵入したことで、政府が機微な政府データ盗難の可能性を懸念していると報じた。サイバー攻撃者は、社会的に工作された E メールで同省職員を攻撃した。その E メールはあたかも 1 人又はそれ以上の信頼された職員から送られたかのごとく装ったものであり、同メールが開かれると悪意のあるソフトウェアが実行され、攻撃者にシステムへのアクセスを許すようになっていた。[154]

152 John Goetz 及び Marcel Rosenbach 共著、「サイバー・スパイ：GhostNet と新たな世界におけるスパイ」、Speigel Online、2009 年 4 月。
153 The Australian Online、「中国外交官はオーストラリアの『サイバー・スパイ』主張を却下、2009 年 4 月。
154 「中国に本拠地を置くハッカーが、南朝鮮財務省イントラネットをアクセス」、AsianPulse News、2009 年 4 月。

主な略号

AMS	Academy of Military Science	軍事科学院
ASAT	Anti-Satellite	対衛星
C2	Command and Control	指揮統制
C4ISR	Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance	指揮・統制・通信・コンピュータ・インテリジェンス・捜索及び偵察
CEME	Complex Electro-Magnetic Environment	複雑な電磁環境
CMC	Central Military Commission	中央軍事委員会
CNA	Computer Network Attack	コンピュータ・ネットワーク攻撃
CND	Computer Network Defense	コンピュータ・ネットワーク防衛
CNE	Computer Network Exploitation	コンピュータ・ネットワーク・エクスプロイテーション
CNO	Computer Network Operations	コンピュータ・ネットワーク作戦
CONUS	Continental United States	米本土
EW	Electronic Warfare	電子戦
GSD	General Staff Department	総参謀部
INEW	Integrated Network Electronic Warfare	統合ネットワーク電子戦
ISR	Intelligence, Surveillance and Reconnaissance	インテリジェンス、捜索及び偵察
IW	Information Warfare	情報戦
NIPRNET	Non-classified Internet Protocol Router Network	非秘密区分指定インターネット・プロトコル・ルーター・ネットワーク
PLA	People's Liberation Army	人民解放軍
TRB	Technical Reconnaissance Bureau	技術偵察局
UAPACOM	US Pacific Command	合衆国太平洋軍
USTRANSCOM	US Transportation Command	合衆国輸送軍

技術用語の解説

バックボーン (Backbone)	主伝送ネットワーク又は一連のネットワークをいい、異なるローカル・エリア・ネットワーク間のデータ伝送に利用される。バックボーンは、一般に接続されるネットワークよりも大きなデータ伝送能力を持っている。インターネット・バックボーンは、主に公共インターネット・ユーザーにデータを転送する政府、商用電気通信及びアカデミック・ネットワークに利用されている高速ネットワークの相互接続を行うものである。
バックドア (Backdoor)	攻撃者が定義した条件下でアクセスできるようにするため、インストールされた正当なソフトウェアを改ざんするか、又は特別仕様のプログラムをインストールすることによって、犠牲となったコンピュータのリモート制御を取り戻す手法をいう。トロイの木馬プログラムやルートキットは、一般にバックドア・コンポーネントを含んでいる。
ブラック・ハット (Black hat)	コンピュータ・ハッカーであって、犠牲対象に対して損害を被らせるか、又は他の認可されていない若しくは不正な活動を行うことに専念する者をいう。
C2 (C2)	コンピュータ・ネットワーク作戦の文脈においては、一般的に危殆化されたコンピュータなどの作戦資産のリモート制御を維持するための通信手段又はそのコンポーネントをいう。
コーダー (Coder)	コンピュータ・プログラマー又はコンピュータ・プログラミング言語コードを記述する者をいう。
コンピュータ・ネットワーク攻撃 (Computer Network Attack: CNA)	コンピュータ・ネットワークを利用し、対象となるコンピュータとコンピュータ・ネットワーク内の情報又はコンピュータとネットワークそれ自身を混乱、妨害、機能低下又は破壊するための攻撃活動をいう。(参照：http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf)
コンピュータ・ネットワーク防衛 (Computer Network Defense: CND)	コンピュータ・ネットワークを利用し、情報システム及びコンピュータ・ネットワーク内における認可されていない活動を防止、監視、分析、検知及び対応する防衛活動をいう。(参照：http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf)

コンピュータ・ネットワーク・エクスプロイテーション (Computer Network Exploitation: CNE)	コンピュータ・ネットワークを利用し、標的又は敵対者の自動情報システム又はネットワークからデータを収集することにより、作戦遂行能力及びインテリジェンス収集能力を与えることをいう。(参照： http://www.dtic.mil/doctrine/jel/new _pubs/jp3_13.pdf)
コンピュータ・ネットワーク作戦 (Computer Network Operations: CNO)	コンピュータ・ネットワーク攻撃、コンピュータ・ネットワーク防衛及びコンピュータ・ネットワーク・エクスプロイテーションから構成される。(参照： http://www.dtic.mil/doctrine/ jel/new_pubs/jp3_13.pdf)
分散サービス妨害 (Distributed Denial of Service: DDoS)	攻撃種類の一つであり、介在する多くのコンピュータが、一つの犠牲となったシステムに対してコンピューティング又は通信資源の完全な消耗をもたらす攻撃を言う。これらの介在攻撃システムは、たいていは予め危殆化され、攻撃者の制御下に置かれている。
電子戦 (Electronic Warfare: EW)	敵を攻撃するため、電磁及び指向エネルギーを利用して電磁スペクトルを制御する軍事活動のすべてをいう。電子戦の主要構成は、電子攻撃、電子防御及び電子戦支援である。
ファイル・トランスファー・プロトコル (File Transfer Protocol: FTP)	ほとんどのウェブ・ブラウザーを含め、FTP サーバーとクライアント・ソフトウェアに実装された標準インターネット・プロトコルをいう。FTP は「信頼性と効率性を兼ね備えたデータ伝送」に利用される。(参照： http://www.rfc-editor.org/ rfc/rfc959.txt)
ハッカー (Hacker)	一個人であり、ベンダーが元々意図したものとは異なる方法でコンピュータ技術を利用する者をいう。 この観点から、ハッカーは次に分類される。 ✧ スクリプト・キディズ(script kiddies)：スキルのない攻撃者であり、新たなぜい弱性又はエクスプロイト・コードを発見する能力がない者をいう。彼らの目標は達成感である。彼らの副目標は、アクセス権を入手しウェブ頁を醜態化することである。 ✧ ワームとウィルス・ライター：ワーム及びウィルスに利用される繁殖コードを作成する攻撃者をいう。しかし、一般的には感染されたシステムへの侵入に利用されるエクスプロイト・コードの作成はしない。彼らの目標は、悪名である。彼らの副目標は、ネットワー

	クとネットワークに接続されたコンピュータ・システムに混乱をもたらすことである。 ✧ セキュリティ研究者とホワイト・ハット・オペレータ：このグループは、バグ・ハンターとエクスプロイト・コーダーの 2 つに分類される。彼らの目標は、利益である。彼らの副目標は、セキュリティを改善し、偉業により感謝されることである。 ✧ 専門的ハッカー―ブラック・ハット：エクスプロイト作成又は実際にネットワークに侵入することにより報酬をもらう個人をいう。このグループも上記と同様の 2 つに分類される。彼らの目標も利益である。(参照：http://www.uscert.gov/control_systems/csthreats.html)
ハイパーテキスト・トランスファー・プロトコル (Hypertext Transfer Protocol: HTTP)	ウェブ・ブラウザーとウェブ・サーバーで利用されるメッセージ・フォーマットとメッセージ交換標準をいう。
ハクティビズム (Hacktivism)	社会的若しくは政治的メッセージの伝達又は政治的若しくは思想的グループの立場を支援するための、意図したコンピュータ・ハッキングをいう。ハクティビズム活動には、データの窃盗、ウェブサイトの醜態化、サービス妨害、リダイレクト[155]、その他が含まれる。
ハクティビスト (Hacktivist)	ハクティビズムを習慣的に行う攻撃者をいう。
インフォコン (INFOCON)	Information Operations Condition(INFOCON)の区分は、防衛準備態勢(Defense Conditions: DEFCON)警報システムに倣ったものであり、INFOCON5～INFOCON1 の 5 段階の漸進的準備態勢からなる統一基準システムである。INFOCON5 レベルの通常準備態勢に始まり、INFOCON1 レベルの最大準備態勢へと、脅威又は攻撃の厳しさにつれレベルが上がる。INFOCON レベルが上がるにつれ、ネットワーク機能又はサービスのエレメントの優先的実施が低くなるか、又は、リスクが高くなればネットワーク機能の一時停止になると思われる[156]。したがって、通常の準備態

[155] リダイレクト：プログラムの入力元や出力先を通常とは異なるものに変更することをいう。

[156] (訳注)：INFOCON の具体的内容については公開されていないことから、このような推量的な表現に

	勢間において利用する CNA ツールは、仮にそれらが利用するサービス又はアプリケーションの機能が停止される場合、無効となる。
情報戦 (Information Warfare: IW)	我自身の情報、情報ベース処理、情報システム及びコンピュータ・ベース・ネットワークを防衛しつつ、彼の情報、情報ベース処理、情報システム及びコンピュータ・ベース・ネットワークに影響を及ぼすことによって、情報優勢を獲得するための軍事行動をいう。(参照 : http://www.jpeocbd.osd.mil/packs/DocHandler.ashx?DocId=3712)
侵入検知システム (Intrusion Detection System: IDS)	観察データと既知又は疑わしい認可されていない活動パターンとのマッチングにより、コンピュータ又はネットワークを監視するシステムをいう。
侵入防止システム (Intrusion Prevention System: IPS)	IDS スタイルのロジックを適用し、ネットワーク・トラフィック、プログラムとデータ・アクセス、ハードウェアの利用などを許可又は拒絶するインライン・システム又はソフトウェアをいう。
ネットワーク振る舞い分析 (Network Behavioral Analysis: NBA)	ネットワーク・トラフィックと既知の許容活動違反に対する警報をモデルにした侵入検知システムをいう。このルールに含まれるものとしては、データ量、時刻、トラフィック率、通信パターン、内容、その他のエレメントがある。
ニップルネット (NIPRNET)	非秘密区分指定のインターネット・プロトコル・ルーター・ネットワーク(Non-classified Internet Protocol Router Network)の略号であり、国防総省のユーザーと機関の間の相互接続は無論のこと、インターネットとのアクセスを提供する国防総省の非秘密区分指定ネットワークをいう。
エヌテーエルエム (NTLM)	アカウント・パスワードに暗号ハッシュ表示を利用するマイクロソフトの認証プロトコルをいう。 (参照：http://msdn.microsoft.com/enus/library/aa378749(VS.85).aspx)
ピーデーエフ (PDF)	Adobe の Portable Document Format(PDF)文書に対するファイル・フォーマットとファイルネーム拡張子をいう。
フィッシング (Phishing)	証明書、銀行口座などの財務情報又はクレジット・カード番号を盗む意図で、犠牲者となる人物をウェブサイトやその他のオンライン資源におびき寄せる策略をいう。フィ

なっていると思われる。

	ッシング攻撃には、一般的に銀行又は電子商取引先などの信頼された実体から送られたと主張する E メールが含まれる。この E メールには、ウェブサイトへのリンクとそのリンクへのクリック指示、及び同ウェブサイトでの実施事項が含まれている。
RAR 又はローシャル・アーカイブ (RAR or Roshal Archive)	より広く利用されている ZIP フォーマットと同じような圧縮ファイル・フォーマットをいい、記憶装置の情報やネットワーク資源を保存するとともに、大きなファイル・セットの移動を簡単にするために利用される。オプションとして、国家標準技術院(NIST)の先進暗号標準アルゴリズムを利用することもできる。ZIP アーカイブスが WinZip (http://www.winzip.com)や zip(http://www.info-zip.org)により作成されるのと全く同じように、RAR アーカイブスも WinRar と RAR(http://www.rarlab.com)によって作成される。
リモート・デスクトップ・プロトコル (Remote Desktop Protocol: RDP)	マイクロソフト・ウィンドウ・コンピュータとアプリケーションに対しリモートからの視認と制御を行うための通信プロトコルをいう。(さらなる詳細情報については次を参照：http://msdn.microsoft.com/enus/library/aa383015(VS.85).aspx)
ルートキット (Rootkit)	ユーザーが認識することなく犠牲となるコンピュータ上にインストールし隠すことができるソフトウェア小片をいう。ルートキットは、大きなソフトウェア・パッケージに含まれているか、又は犠牲となったマシン上のぜい弱性を利用することができる攻撃者によってインストールされる。攻撃者は、検知されることなく、標的となったコンピュータ上の情報のアクセス、ユーザーの行為のモニタ、プログラムの改ざん、又はその他の活動を行うことができる。(参照：http://www.us-cert.gov/cas/tips/ST06-001.html)
セキュリティ事象及び情報管理 (Security Event and Information Management: SEIM)	ファイアウォール、IDS/IPS、ウィルス対策ソフトウェア、認証システムなどの多くの異なるシステムからのセキュリティ事象に対する中央集権化された収集と管理をいう。SEIM は、一コンポーネント・システムだけでは容易に識別できない振る舞いパターンの警報を発するよう、複雑な複数要素のルールを設定することができる。
スピア型フィッシング	選定された犠牲者のグループを攻撃目標とするフィッシ

(Spearphishig)	ング攻撃をいう。たいていは、一つの会社、学校、企業などが選定される。「スピア型フィッシング」は、一般には標的を定めた E メール攻撃のすべてをいい、フィッシングの範疇に限定されるものではない。
トロイの馬 (Trojan horse)	(プログラムを走らせている)ユーザーの権限を悪用することができる隠された機能をもつ、(実際はともかく)外見上は効果的なプログラムをいい、(実行されると)セキュリティ脅威をもたらすことになる。トロイの馬は、プログラム・ユーザーが意図しない動作をする。トロイの馬のインストールは、ユーザーによるか、又は他の手段により、認可されていないアクセス権を得た侵入者によることもある。侵入者がトロイの馬を利用してシステムの破壊を企てる場合、それが成功するためには他のユーザーがそのトロイの馬を走らせていなければならない。(参照：http://www.cert.org/ advisories/CA-1999-02.html)
トンネリング (Tunneling)	一つの通信データ・ストリームを他のものの内部に閉じ込め、閉じ込められたものを元に戻す技法をいう。攻撃者は、ネットワーク境界を通過することが許可されていないネットワーク・プロトコルを通過させるため、トンネリングを頻繁に利用する。これにより、境界防衛を打ち破ることができる。(参照：http://www.its.bldrdoc.gov/projects/devglossary/_tunneling.html)
2 要素認証 (Two-factor Authentication: T-FA)	現存する認証手法には、3 つの基本的な「要素」が含まれている。 1. ユーザーが知っている何か(例：パスワード、PIN) 2. ユーザーが持っている何か(例：ATM カード、スマート・カード) 3. ユーザーである何か(例：指紋などの生物学的特性) T-FA は、ユーザーに対して 3 つの可能要素の中から 2 つを求め、これらを認証メカニズムの入力とする。ある T-FA システムにおいて知られている欠点は、スマート・カード又はトークン上に含まれている証明書のハッシュ換算データをサーバーに記憶していることである。これが攻撃者の手中にあれば、攻撃者はそのデータを認証システム上で再生することができる。この場合、プロキシ・サーバーは、物理的なカード又はトークンを必要としない。(参照：

	http://www.ffiec.gov/pdf/authentication_guidance.pdf)
合衆国太平洋軍 (USPACOM)	合衆国太平洋軍(United States Pacific Command: USPACOM)は、合衆国軍の 6 つの統合軍のうちの一つであり、その管轄地域は合衆国西海岸からインドの西側国境、そして南極大陸から北極に及ぶ。同軍の現在の兵員数は約 325,000 である。
合衆国輸送軍 (USTRANSCOM)	合衆国輸送軍(United States Transportation Command: USTRANSCOM)は、軍事作戦のすべての分野における共同一貫輸送を行う。USTRAMSCOM は、3 つの輸送軍から構成されている。それらは、空軍航空軌道軍団、陸軍配備流通軍及び海軍軍事海上輸軍である。
ゼロデイ・エクスプロイト (Zero day Exploit)	ソフトウェア維持ベンダーが未着手のソフトウェアぜい弱性に対する攻撃をいう。その問題に対する解決策が固まるまで、ベンダーによる公表がないのが一般的である。したがって、これらの攻撃を検知するのは困難となり、犠牲者は攻撃にさらされているのを認識しない状態に置かれる。

参照文献

(1) Anderson, Robert H, Feldman, Phillip M., et al., Securing the U.S. Defense Information Infrastructure, RAND Corp., 1999.

(2) Aning, Jerome and Olchondra, Riza T., RP Gov't Websites Vulnerable to Hacking, Philippine Daily Inquirer, March 31, 2009, http://technology.inquirer.net/infotech/infotech/view/20090331-197122/RP-govtwebsites-vulnerable-to-hacking#

(3) Asian News International, "French Embassy Website in China Hacked," ZeeNews, December 12, 2008, http://www.zeenews.com/news490316.html

(4) AsiaPulse News, "China-Based Hackers Access S. Korean Finance Ministry's Intranet," April 8, 2009, http://www.highbeam.com/doc/1G1-197405142.html

(5) Ball, Desmond, "Signals Intelligence in China" Jane's Intelligence Review, August 1, 1995.

(6) Blasko, Dennis J., The Chinese Army Today, Routledge, 2006.

(7) Bliss, Jeff, "China's Spying Overwhelms U.S. Counterintelligence," Bloomberg, April 2, 2007, http://www.bloomberg.com/apps/news?pid=20601087&sid=ab2PiDl1qW9Q&refer=home

(8) Bristow, Damon, "Cyber-warfare rages across Taiwan Strait," Jane's Intelligence Review, Vol 12, Issue 2, February 1, 2000.

(9) Cheng, Dean, "PLA Views on Space: The Prerequisite for Information Dominance," Center for Naval Analysis, CME D0016978.A1, October 2007

(10) Christensen, Thomas J., "Windows and War: Trend Analysis and Beijing's Use of Force," in New Directions in the Study of China's Foreign Policy, Alastair Iain Johnston and Robert Ross, eds. Stanford University Press, 2006.

(11) Cui Yafeng, "On Changes in Relationship Strategy Has With Campaigns and Battles in Modern Warfare", China Military Science, December 29, 2008, Translated by OSC, CPP20081229563002.

(12) Dai Qingmin, "On Seizing Information Supremacy," China Military Science, April 20, 2003, No 2, Vol. 16, pp 9-17, Translated by OSC, CPP20020624000214.
—"On Integrating Network Warfare and Electronic Warfare," China Military Science, February 1, 2002, pp 112-117, Translated by OSC, CPP20021062400024.

(13) Blakely, Rhys, Richard, Jonathan, Rossiter, James and Beeston, Richard, "MI5 Alert on China's Cyberspace Spy Threat," The Times, December 1, 2007, http://business.timesonline.co.uk/tol/business/industry_sectors/technology/articl

(14) e2980250.ece
(15) Chickowski, Ericka, “Naval War College Network Shuts Down After Chinese Attack,” SC Magazine, December 9, 2006, http://www.scmagazineus.com/Naval-War-College-network-shuts-downafter-Chinese-attack/article/34305/
(16) Elegant, Simon, “Enemies at the Firewall,” Time Magazine, December 6, 2007, http://www.time.com/time/magazine/article/0,9171,1692063,00.html
(17) Epstein, Keith and Elgin, Ben, Network Security Breaches Plague NASA, usiness Week, November 20, 2008. ttp://www.businessweek.com/magazine/content/08_48/b4110072404167.htm
(18) Fan Li , "Exploration of Construction of Security Defense Architecture for Military Information System;" Computer Security, February 1, 2009 pp 90, Translated by OSC, CPP20090528670007.
(19) Faiola, Anthony, “Cyber Warfare: China vs. Japan,” MSNBC News, May 11, 2005, http://www.msnbc.msn.com/id/7796346/
(20) Ferster, Warren and Clark, Colin, “NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft,” by, Space News Business Report, October 3, 2006, http://www.space.com/spacenews/archive06/chinalaser_1002.html
(21) Fisher, Richard Jr., “People’s Liberation Army Leverage of Foreign Military Technology,” March 22, 2006, International Assessment and Strategy Center, http://www.strategycenter.net/research/pubID.97/pub_detail.asp.
(22) Gartzke, Ulf, “Outrage in Berlin Over Chinese Cyber Attacks,” The Weekly
(23) Standard, August 31, 2007, http://www.weeklystandard.com/weblogs/TWSFP/2007/08/outrage_in_berlin_over_chinese.asp
(24) Goetz, John and Rosenbach, Marcel, “Cyber Spies: ‘GhostNet’ and the New World of Espionage,” Der Speigel Online, April 10, 2009, http://www.spiegel.de/international/world/0,1518,618478,00.html
(25) Gong Gucheng, “Information Attack and Information Defense in Joint Campaigns," Military Art Journal, October 1, 2003, Translated by OSC, CPP20080314623007.
(26) Grow, Brian, Epstein, Keith, Chi-Chu Tschang, “The New E-spionage Threat,”
(27) BusinessWeek, April 10, 2008, http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm
(28) Harris, Shane, “China’s Cyber-Militia,” The National Journal, May 31, 2008, http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php

(29) Henderson, Scott, The Dark Visitor, January 2007.
(30) Hess, Pamela, “China Prevented Repeat Cyber Attack on US,” UPI, October 29, 2002.
http://www.upi.com/Business_News/Security-Industry/2002/10/29/Chinaprevented-repeat-cyber-attack-on-US/UPI-88751035913207/
(31) Homeland Security Newswire, China Suspected in Hacking Attempt on Oak Ridge National Lab, December 10, 2007;
http://homelandsecuritynewswire.com/single.php?id=5198
(32) Singh, Gurmukh, “Chinese Hack Into Indian Embassies, Steal Dalai Lama’s Documents,” IANS, March 2009,
http://www.thaindian.com/newsportal/scitech/chinese-hack-into-indian-embassies-steal-dalai-lamasdocuments_100172617.html
(33) Information Office of the State Council of the People's Republic of China, China's National Defense in 2004,, Beijing, 27 December 2004.
http://english.peopledaily.com.cn/whitepaper/defense2004/defense2004.html
(34) —China's National Defense in 2006, December 29, 2006,
http://english.chinamil.com.cn/site2/news-channels/2006-12/29/content_691844.htm
(35) —China's National Defense in 2008, January 20, 2009,
http://www.chinadaily.com.cn/china/2009-01/20/content_74133294.htm
(36) Jane's Sentinel Security Assessment, “China and Northeast Asia,” April 3, 2009.
(37) Johnston, Alastair Iain, “China’s Militarized Interstate Dispute Behavior 1949-1992:
(38) A First Cut at the Data,” The China Quarterly, 1998, No.153 (March 1998).
(39) Kamphausen, Roy and Scobell, Andrew, eds., Right Sizing The People’s Liberation Army: Exploring The Contours Of China’s Military, Strategic Studies Institute, September 2007.
(40) K'an Chung-kuo, "Intelligence Agencies Exist in Great Numbers, Spies Are Present Everywhere; China's Major Intelligence Departments Fully Exposed, Chien Shao, No 179, January 1, 2006, Translated by OSC, CPP20060110510011.
(41) Ke Zhansan, “Studies in Guiding Ideology of Information Operations in Joint Campaigns,” China Military Science, April 20, 2003, Translated by OSC, CPP2003728000210.
(42) Lague, David, “Chinese See Military Dependence on Computers as Weakness,” The New York Times, August 29, 2007,
http://www.nytimes.com/2007/08/29/world/asia/29iht-cyber.1.7299952.html

(43) Liao Wenzhong, "China Military Net Force: National Security, Public Security, and the People's Liberation Army," Ch'uan-Ch'iu Fang-Wei Tsa-Chih , March 2007, Translated by OSC, CPP20071023318001.
(44) Li Deyi, "A Study of the Basic Characteristics of the Modes of Thinking in Informatized Warfare," China Military Science, August 20, 2007, pp 101-105, Translated by OSC, CPP20081028682007.
(45) Li Zhilin, "On the Trend of Changes in Operations Theory Under Informatized Conditions," November 12, 2008, Translated by OSC, CPP20081112563002.
(46) Lu Qiang, "Zhuoyan Xinxihua Zhanzheng Tedian Jiaqiang Chengshi Minbing Jianshe," (Focus On The Characteristics Of Information Warfare To Strengthen The City Militia Construction), China Militia Magazine, August 2003, http://www.chinamil.com.cn/item/zgmb/200308/txt/16.htm
(47) Marquand, Robert and Arnoldy, Ben, "China Emerges as Leader in Cyberwarfare," The Christian Science Monitor, September 14, 2007, http://www.csmonitor.com/2007/0914/p01s01-woap.html
(48) McMillan, Robert, US Defense Department Under Cyber Attack, IDG News Service, June 2007.
(49) Medeiros, Evan, Cliff, Roger, Crane, Keith, Mulvenon, James, A New Direction for China's Defense Industry, RAND Corp, 2005.
(50) Melvin, Ellis L., A Study of The Chinese People's Liberation Army Military Region Headquarters Department Technical Reconnaissance Bureau, June 19, 2005.
(51) "Minbing Wangluo Zhan Fendui Zhize" (Duties of the Network Warfare Militia Unit), March 16, 2008. http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp?infoNo=26366
(52) Minnick, Wendell, "Taiwan Faces Increasing Cyber Assaults," Army Times Publishing, June 12, 2006, http://minnickarticles.blogspot.com/2009/09/taiwanfaces-increasing-cyber-assaults.html
(53) Moore, Malcolm, "China's Global Cyber-Espionage Network GhostNet Penetrates 103 Countries," Telegraph.co.uk, March 29, 2009, http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-globalcyber-espionage-network-GhostNet-penetrates-103-countries.html
(54) Mount, Mike, Hackers Stole Data on Pentagon's Newest Fighter Jet, CNN, April 21, 2009, http://www.cnn.com/2009/US/04/21/pentagon.hacked/index.html
(55) Mulvenon, James, "PLA Computer Network Operations: Scenarios, Doctrine,

Organizations, and Capability," in Beyond the Strait: PLA Missions Other Than Taiwan, Roy Kamphausen, David Lai, Andrew Scobell, eds., Strategic Studies Institute, April 2009.

(56) Norton-Taylor, Richard, "Titan Rain – How Chinese Hackers Targeted Whitehall," The Guardian, September 5, 2007, http://www.guardian.co.uk/technology/2007/sep/04/news.internet

(57) Onley, Dawn and Wait, Patience, "Red Storm Rising: DoD's Efforts to Stave Off Nationn-State Cyberattacks Begin with China," Government Computer News, August 17, 2006, http://www.gcn.com/Articles/2006/08/17/Red-stormrising.aspx

(58) Peake, Ross, "Australia Confirms Cyber Attacks, Canberra Times," August 3, 2008, ttp://www.canberratimes.com.au/news/local/news/general/australiaconfirms-cyber-attacks/510016.aspx

(59) Peng Guangqiang and Yao Youzhi, eds, The Science of Military Strategy, Military Science Publishing House, English edition, 2005.

(60) Schwankert, Steven, "US Congressmen Accuse China of Hacking Their Computers," IDGNS, June 12, 2008, http://www.infoworld.com/archive/200806?page=46

(61) Sevastopulo, Demetri, "Hackers Breach White House System," The Financial Times, November 6, 2008, http://us.ft.com/ftgateway/superpage.ft?news_id=fto110620081938360726&page=2

(62) Sevastopulo, Demetri, Cyberattacks on McCain and Obama Team's 'Came from China', The Financial Times, November 6, 2008.

(63) Shi Zhihua, Basic Understanding of Command of Information Operation," China Military Science, No. 4, 2008, Translated by OSC, CPP20090127563002.

(64) The Straits Times, "Chinese Plan to Hack into Taiwan Websites," October 10, 2000, http://www.hartford-hwp.com/archives/55/105.html

(65) Stokes, Mark A, China's Strategic Modernization: Implications for the United States, U.S. Army Strategic Studies Institute, September, 1999.

(66) Tamura, Hideao and Soma, Masaru, "Japan Increasingly 'Susceptible to Cyber Attacks from Chinese PLA," Tokyo Sankei Shimbun, October 2007.

(67) Tang, Rose, "China Warns of Massive Hack Attacks," CNN, May 3, 2001, http://archives.cnn.com/2001/WORLD/asiapcf/east/05/03/china.hack/

(68) Thornburgh, Nathan, "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them," Time Magazine, August 29, 2005, http://www.time.com/time/magazine/article/0,9171,1098961,00.html

(69) Tung, Liam, “China Accused of Cyberattacks on New Zealand,” CNET News, September 13, 2007, http://news.cnet.com/China-accused-of-cyberattacks-on-New-Zealand/2100-7348_3-6207678.html
(70) US China Economic and Security Review Commission, 2007 Report to Congress, November 2007, http://www.uscc.gov
(71) US Department of Defense, Annual Report to Congress: Military Power of the People’s Republic of China 2006, May 2006.
(72) —Annual Report to Congress: Military Power of the People’s Republic of China
(73) 2009, March 2009. —Joint Publication 4-0: Joint Logistics, 18 July 2008, http://www.dtic.mil/doctrine/jel/new_pubs/jp4_0.pdf
(74) US Pacific Command, Virtual Information Center, “People’s Republic of China Primer,” August 4, 2006, http://www1.apaninfo.net/Portals/45/VIC_Products/2006/08/060804-P-China.doc
(75) Wang Houqing, Zhang Xingye, Huang Bin, and Zhan Xuexi, eds, The Science of Campaigns, National Defense University Publishing House, May 2000, Translated by OSC, in CPP20010125000044.
(76) Whiting, Allen S., “China’s Use of Force 1960-1996, and Taiwan,” International Security, Vol. 26, No. 2, Fall, 2001.
(77) Ye Youcai and Zhou Wenrui, "Building a High-quality Militia Information Technology Element" National Defense, September 15, 2003 pp 45, Translated by OSC, CPP20031002000138.
(78) “Yongning is the First to Set Up Information Warfare Militia Units,” March 19, 2008, http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp
(79) Zhu Jianjian and Li Lijian, “Memorandum on National Defense Reform and Innovation (Part 5): Website Established by Ezhou Militia," National Defense, May 2001, Translated by OSC CPP20090102670001.

米中経済安全保障調査委員会議会報告 2009 から抜粋

第 2 章：合衆国の安全保障利益に直接影響を及ぼす中国の活動

第 3 節：合衆国を攻撃目標とした中国の人的スパイ活動と合衆国国家安全保障に及ぼす影響

第 4 節：合衆国を攻撃目標とした中国のサイバー活動と合衆国国家安全保障に及ぼす影響

本委員会の調査及び報告範囲は次のとおりである。

「**地域経済及び安全保障への影響**―合衆国、台北及び中華人民共和国（軍の近代化及び中華人民共和国の対台北軍事力展開を含む）三者間の経済及び安全保障の関係、中華人民共和国の国家予算、並びに中華人民共和国内の不安定状態及びこのような内部不安定状態に起因する問題の外面化兆候に関連する中華人民共和国の財政力・・・・・」

目　次

第２章　合衆国の安全保障利益に直接影響を及ぼす中国の活動
第３節　合衆国を攻撃目標とした中国の人的スパイ活動と合衆国国家安全保障に及ぼす影響

１　序論

司法省は最近、増大する中華人民共和国(People's Republic of China: 中国)関与のスパイ行為又は不正な技術取得に係る事件を提起した。これらの提起の中には報道の大見出しとなった派手なスパイ事件もあるが、大部分は輸出規制法違反又は企業スパイに係る事件である。それらの事件は大衆の注意を引くことはないが、合衆国の経済と国家の安全保障にとっては極めて重大な事件なのである。

元連邦捜査局(Federal Bureau of Investigation: FBI)カウンターインテリジェンス部の副部長 David Szady は、中国を「今日の合衆国に対する最も巨大なスパイ脅威である」と言っている。FBI 長官 Robert Mueller は、「中国は、軍事技術ばかりでなく、経済力の面でも前に出ようとして、我々の秘密を盗んでいる」と警告した。これは重大な脅威である。元国家カウンターインテリジェンス行政部主席カウンターインテリジェンス職員 Joel Brenner は、中国のインテリジェンス機関を、合衆国の攻撃目標に侵入しようとする 140 の組織の中で最も積極的であると述べている。

政府カウンターインテリジェンス当局者によるこの他の声明は、中国のインテリジェンス収集活動がその規模、強烈さ及び複雑さの点で増大していることを示唆している。国家インテリジェンス局の 2009 年 5 月の声明によれば、カウンターインテリジェンス・コミュニティは、中国が機微な合衆国企業機密や技術だけでなく、合衆国の軍事、政治及び経済に係る秘密を攻撃目標としている最も積極的な国であるとしている。「我々は、多くの理由から、現在の中国は冷戦時代の外国のインテリジェンス脅威に比べ、相当大きな脅威をもたらしていると確信している」

中国関連の法の執行に係るほとんどの事件は、合衆国規制技術の違法な取得に関係したものである。これらの事件の中には中国のインテリジェンス機関に結びついているものもあるが、ほとんどの事件は他の国家機関に結びついており、とりわけ中国の軍事産業複合体の工場や研究所が顕著なものとなっている。司法省が発表したデータによれば、2007 年度及び 2008 年度間の連邦裁判訴追に至った事件において、中国はイランに次ぐ第 2 位の合衆国規制技術の主要な違法輸出先となっている。これらの事件で中国に違法に輸出された具体的な技術としては、ロケット打ち上げデータ、スペース・シャトル技術、ミサイル技術、海軍軍艦データ、無人航空機技術、熱画像システム、軍暗視システムなどがある。

本年、米中経済安全保障調査委員会は、中国の対合衆国スパイ行為について、合衆国国家安全保障や将来の合衆国経済競争力への影響は無論のこと、それらスパイ行為の大きさについても調査した。中国の複数の国家組織が、活発な合衆国規制技術取得活動に関与しており、中国政府も民間企業が政府に代わって技術を取得する活動を奨励し、報酬を与えている。さらに、中国政府のエージェントが合衆国政府職員に報奨金をいとわず提供し、

彼らに秘密区分指定情報を危うい状態に至らしめるよう促していることがますます表面化している。最後に、中国政府当局は、合衆国内の中国反体制派組織に対する監視といやがらせを行っている。

補足的な分析は、本委員会 2009 議会報告の秘密区分指定付録に掲載されている。中国の広範囲にわたるますますのサイバー・スパイ活動については、本報告書第 2 章第 4 節「合衆国を攻撃目標とした中国のサイバー活動と合衆国国家安全保障に及ぼす影響」を参照されたい。

２　中国の伝統的なインテリジェンス手法

伝統的な中国のスパイ行為アプローチは、合衆国が過去に奨励した「古典的な」スパイ行為アプローチとは相当異なっている。一般的に、中国は、外国の情報源が関与している場合、「通常は情報に対する報酬をエージェントに支払うことなく、そのエージェントに秘密区分指定文書の提供を要求するか又は諜報部員を使ってそのエージェントから情報を引き出すか若しくは『デッド・ドロップ』[157]のような密かな活動を行う。・・・中国は、一度に少しずつの情報を取得することを好む」　このような情報の取得方法に含まれるものに、外国の科学専門家を中国主催のカンファレンスに招待すること、彼らを誉めそやすこと、精神的に疲れさせるためへとへとに疲れさせるスケジュールにさらすこと、絶え間のない連携された聞き出しを浴びせ、スパイ行為を意識させることなく不注意な開示をさせてしまうことなどがある。

ロシアの諜報部員は自尊心、意地汚い欲望、その他の人的弱みを利用することに目を向けるが、中国の諜報部員はロシアの諜報部員とは異なり、「中国の友人」として好んで活動する好ましい人物を利用する傾向がある。このような傾向は、中国が攻撃目標にした中国系アメリカ人のリクルートに最も明確に見られる。また、中国のエージェントは、情報源として他の民族的背景を持つ合衆国市民も利用している。

２.１　従来の情報源リクルート慣行からの変化

中国が指示した合衆国へのスパイ行為に係る歴史的事件の多くに、中国の民族的文化遺産を引き継いた合衆国市民が関与している。このことに関する論点は、中国系アメリカ人が他の民族的背景を持つ合衆国市民に比べ信頼性に乏しいということではない。元 FBI の分析家 Paul Moore はかつて、「中国のインテリジェンス問題で常に華僑が関与していると思われるその理由は、中国がいつも支援を求める人物が単に彼らであったにすぎないということだ」と言及した。

合衆国政府のカウンターインテリジェンス関連のハンドブックは、次のように説明している。

---

157 訳注：dead drop。スパイの連絡情報の隠し場所をいう。

通常の中国のリクルート活動の際の売込みポイントのすべては、民族性それ自体をアピールすることではなく、攻撃目標にされた人物が中国、中国に住んでいる家族、中国の旧友などに対して抱いている義務感である。中国のアプローチの最も重要な点は、その人物の弱点を利用することではなく、中国を助けたいというその人物の望みを何らかの方法でアピールすることである。・・・義務感を誘発させるための民族的背景を利用した標的行為は、中国のインテリジェンス活動において唯一他との違いを示す最も特徴的な行為である。

とはいえ、本委員会は、中国のスパイ行為に係るこれらの歴史的慣行からの変化に関し、昨年合衆国内において発生した中国関連の少なくとも 2 件の顕著なスパイ行為事件については、中国のインテリジェンス機関が、情報と引き換えに金銭的報酬を与えることにさらなる意欲を示すだけでなく、中国系アメリカ人コミュニティの範囲を超えて、情報源を捜し求めていたことをあらわにした点に注目している。（本節の後半に述べる「Bergersen と Fondren 事件」を参照）

３　中国のインテリジェンスと技術情報の収集家

３.１　国家安全部

国家安全部(Ministry of State Security)[158]は、中国の主要な文民インテリジェンス機関であり、国外インテリジェンス活動及び国内保安活動の両責任を負っている。中国の国家安全部は、他の共産主義国家のインテリジェンス機関と同様に、中国共産党(Chinese Communist Party: CCP)支配の片腕として最もよく知られている。その委ねられた主要な任務は、中国共産党の政治的権力を維持することであり、国外におけるインテリジェンスの収集活動である。この他にも、政治的用語の広義の解釈に立脚したカウンターインテリジェンス活動における指導的役割も担っている。この広義のカウンターインテリジェンス活動には、政治的反体制派や民族分離独立派などの中国共産党の敵対者と見られるグループに対する監視と鎮圧が含まれている。また、この内部の「敵対性要素」に対する活動の役割は、海外に対しても向けられている。報道によれば、元国家安全部高官であり、その後合衆国に定住を余儀なくされた Li Fengzhi は 2009 年当初、国家安全部の海外活動における主要な力点は、中国反体制派と民主主義擁護グループに対する標的行為であると明言した。

国家安全部の海外におけるインテリジェンス活動は、もっぱら同部第二局が行っており、公式の外交官によるスパイとしての身元偽装（official diplomatic cover)と学生やビジネ

158訳注：我が国で考えると中華人民共和国政府の「省」ということになるが、中国では「部」と表現していることから、敢えて「部」とした。なお、中国の同部のウェブサイトにおいても、中国語表現は「国家安全部」、英語表現は「Ministry of State Security」となっている。

スマンなどの非公式なスパイとしての身元偽装（unofficial cover)の両者を含む広範な身元偽装の下に、海外のエージェントを操っている。また、国家安全部は、ニュース報道記者としての身元偽装も広範囲に利用しており、エージェントを中国国営通信社新華社の特派員及び人民日報や中国青年報などの報道記者として海外に派遣している。

さらに、国家安全部は、国際的面目を同部所属のシンクタンクの形で北京北西部に位置する中国現代国際関係研究院(China Institute for Contemporary International Relations: CICIR)に保っている。CICIR は、その公共的役割は別として、国家安全部第 8 局として完全に組み入れられており、中国の指導者に対する研究及び分析活動を行っている。さらに、CICIR は自身の機関誌「現代国際関係」を出版するとともに、しばしば合衆国訪問者の接待を行っている。本米中経済安全保障調査委員会のメンバーは、中国における年次の委員会事実調査出張時に、CICIR の代表と複数回にわたって面談している[159]。（CICIR 及び中国のシンクタンクと合衆国の団体との関係の詳細については、本報告書の第 4 章第 2 節「中国の外部宣伝と感化活動及びそれに伴う合衆国安全保障への影響」を参照されたい）

３.２　人民解放軍のインテリジェンス機関

中国軍のインテリジェンス機関は、人民解放軍(People's Liberation Army: PLA)総参謀部第 2 部であり、軍事情報部としても知られている。軍の一組織としての軍事情報部は、主に外国軍の戦力組成、軍事ドクトリンや兵器システムに係るインテリジェンス収集を行っている。軍事情報部は、中国大使館武官による公然の情報収集だけでなく、身元偽装のエージェント活動によっても公然と収集活動を実施している。

軍事情報部は、1990 年代からの情報によれば、外国の技術、とりわけ軍事技術への適用可能性がある技術の取得に当たって、最も積極的に活動した中国のインテリジェンス機関であるとされている。軍事情報部は、技術移転やその他のインテリジェンス活動を促進させるため、複数のフロント・カンパニーを香港で経営している。

また、軍事情報部は、国家安全部と同様に、同部所属のシンクタンク機関を保持している。軍事情報部の対外政策と国家安全保障問題を取り扱うシンクタンクは、中国国際戦略研究所(China Institute of International Strategic Studies: CIISS)である。もっとも、CIISS がその上位組織である軍事情報部に結びついていることは公にされていないが、大部分の研究者は現又は元 PLA の将校である。CIISS に配属された現役将校は、研究所と軍事情報部の任務に分けられている。同研究所の現所長は、元軍事情報部部長であった退役陸軍大将 Xiong Guangkai である。本委員会のメンバーは中国への事実調査訪問時に、CIISS の代表と話し合いの場を持った。また、軍事情報部は、南京にある PLA の国際関

159 訳注：我が国の「シンクタンク 2005・日本」は 2007 年 7 月 25 日、CICIR の雀立如院長や研究者と意見交換を行った、と同シンクタンクのウェブサイトに掲載されている。
(http://www.tt2005.jp/modules/news/article.php?storyid=72)

係研究所と直接関係している。同研究所は、軍事情報部の将校訓練センターとしての役割を果たしている。

次に示す表は、包括的なものではないが、中国のインテリジェンス収集機関、その上位組織、それらの主要任務を示したものである。

インテリジェンス機関	上位組織	主要任務
文民組織		
国家安全部	中国国務院/CCP 政治局政治法律委員会	✧ 外国のインテリジェンス収集 ✧ インテリジェンス分析 ✧ カウンターインテリジェンス ✧ 反体制派グループの鎮圧
公安部	中国国務院/CCP 政治局政治法律委員会	✧ 国内治安活動/法の執行 ✧ カウンターインテリジェンス
CCP 対外連絡部	CCP 中央委員会	✧ 外国の政党との連絡 ✧ 感化活動 ✧ インテリジェンス収集
CCP 統一戦線部	CCP 中央委員会	✧ 非共産主義中国人グループとの連絡 ✧ 感化活動 ✧ インテリジェンス収集
様々な文民科学研究開発機関	中国科学アカデミー(主)	✧ 技術取得
軍事組織		
PLA 総参謀部第 2 部(軍事インテリジェンス)	PLA 総参謀部	✧ 外国のインテリジェンス収集(特に軍事データ) ✧ インテリジェンス分析 ✧ 技術取得
PLA 総参謀部第 3 部(シグナル・インテリジェンス)	PLA 総参謀部	✧ シグナル・インテリジェンス収集と分析 ✧ サイバー・インテリジェンス収集と分析
PLA 総参謀部第 4 部	PLA 総参謀部	✧ 電子戦(ジャミングなど) ✧ コンピュータ・ネットワーク攻撃
PLA 総政治部国際連絡部	PLA 総政治部	✧ 外国のインテリジェンス収集 ✧ 政治戦/心理戦
様々な防衛関連企業	11 の国有会社	✧ 技術取得

(出典：複数の情報源に基づき、本委員会がまとめたものである)

３.３　その他のインテリジェンス組織

中国政府は、上記の他にも外国のインテリジェンス収集活動に関与する多くの制度上の組織を持っている。人民解放軍(PLA)総参謀部第 3 部は、中国の第一級のインテリジェンス収集機関であり、伝えられるところによれば、中国の全インテリジェンス機関の中でも最大の機関とされている。もっとも、第 3 部の総人員数については、権威のあるオープン・ソースから入手することはできなかった。この第3部は、電子戦任務が付与されているPLA総参謀部第 4 部との補完関係にもある。（第 3 部及び第 4 部の活動詳細については、本報告書第 2 章第 4 節を参照されたい）

PLA 総政治部の国際連絡部は、国防部及び軍事情報部とともに合衆国に対しあからさまなインテリジェンス収集活動を行う中国三大機関の一つである、と合衆国政府のカウンターインテリジェンス・ハンドブックに明示されている。この国際連絡部には、宣伝活動と心理戦の任務が付与されており、台湾軍将校を攻撃目標に過去数年間多忙な活動を実施している。もっとも、同組織の合衆国内における活動について公に入手できる情報がほとんどないこともあって、同組織の合衆国内での活動は、国防部又は軍事情報部のいずれよりも小規模で、強い印象を与えていないと言われている。しかしながら、2009 年 5 月の合衆国国家インテリジェンス局の発表によると、国際連絡部は合衆国大企業に対する活発な収集家であるとして、リストアップされている。

中国共産党(CCP)のその他の組織も、外国のインテリジェンスの収集と政府の代理としての宣伝活動の役割を担っている。これらの組織には、中国共産党の統一戦線部と中国共産党の対外連絡部が含まれている。中国の公式通信社である新華社も、インテリジェンス機関のある機能を担っており、国内及び国際の大事件情報を収集し、秘密区分指定報告文書を作成の上、中国の指導者に提出している。

４　中国の合衆国内におけるインテリジェンスと技術情報の収集

最近の犯罪起訴に係る情報は、合衆国内における中国のインテリジェンス及び技術情報収集活動が、以前に認識されていたものに比べ、より変化に富み、かつ、複雑化していることを示唆している。中国政府に代わって情報と技術の収集を行う活動家の範囲は、上記に述べた専門的なインテリジェンス機関のエージェントから、技術やデータを探し出して中国機関に売却することができる人物に及んでいる。これらの活動は、4 つに大別することができる。①「保険統計的(actuarial)」：複数の情報源からの寄せ集めで取り繕った保険統計的インテリジェンス、②「専門的」：中国のインテリジェンス・エージェントによって実施又は直接後援を受けた専門的インテリジェンス収集、③「組織の指示」：中国国家の科学技術開発と軍事企業セクター組織からの指示に基づく規制技術の取得、及び④「請負人」：個人の収集家であり、中国政府からの報酬を求める企業スパイと不正技術取得

４.１「保険統計的インテリジェンス」

中国のスパイ行為に特有な要素は、「砂粒(grain of sand)」又は「保険統計的(actuarial)」インテリジェンス収集アプローチである。中国のインテリジェンス活動は、ある特定の規制情報に的を絞って収集するよりも、膨大な量の生の情報をかき集めるのが一般的である。そのほとんどは、秘密区分指定情報でも又は規制情報でもなく、完全に無関係の情報かもしれない。そして、それらの膨大なパズル片を組み合わせた「モザイク」から新事実を明らかにする。元 FBI 特別捜査官の I.C. Smith は、この伝統的なアプローチは「単に我々のために情報を入手せよ。我々が後で選り分ける」というものである、と本委員会に語った。

また、中国のインテリジェンス部員は、誰か十分な信頼を置ける人物よりも多くのエージェント又は情報源から情報をかき集めるというアプローチも見せている。「すべてのプロセスは、時には『保険統計的インテリジェンス』と言われることがある。なぜなら、その基本は、保険会社の保険計理人が大きなグループの人々を対象にした保険を引き受ける際に、その利益性の決定に当たって適用する原則とは異なるからである」　この保険統計的アプローチは、複数の情報源からの情報に基づくクロス・チェックを可能にするものであるが、一方ではいかなる特殊例における否認性をも増大させ、いかなる危険性に対してもリスクを低減させる、というものである。

この伝統的な中国のインテリジェンス収集手法は、合衆国法廷に起訴できる明白なスパイ行為の証拠を作成するための「古典的」モデルとは若干異なる。中央情報局(Central Intelligence Agency: CIA)や FBI の議会報告書が特徴付けるように、中国のスパイ活動は「一般的に控えめであるが本質的に非凡であることから、FBI に対して相当なカウンターインテリジェンス上のジレンマをもたらしている」　そして、この中国のアプローチは非効率的なように見えるが、これまでに相当な成果をもたらしている。合衆国カウンターインテリジェンス・ハンドブックの中に、記憶すべき警句として、伝統的な中国のスパイ行為アプローチは「非効率的であるが、非効果的ではない」というのがある。

CIA と FBI 共同による秘密区分指定解除の 2000 年版報告書は、中国の技術開発レベルが西側諸国に比べ低いことから、「砂粒」アプローチによる収集の普及がある程度説明できると示唆している。

> 中国の収集プログラムは、中国自身が開発途上の「キャッチアップ」状況にあると考えていることから、比較的広範囲なものとなっている。中国の収集家は、中国にとって価値のあるものならどのような情報や技術でも攻撃目標にしている。したがって、規制情報、企業機密情報や秘密区分指定情報だけでなく、オープン・ソースの情報も求めることとなる。

しかしながら、最近における中国の急速かつ劇的な科学技術の発展は、このようなやみ

くもな収集手法を少しずつ減少させているようである。中国の科学研究開発と企業セクターがより発展するにつれ、彼らの不足分野も明らかとなるはずである。したがって、彼らの収集要求事項も、より集中した特定分野にシフトするものと思われる。中国の国家又は組織が指示した情報と技術の取得に関する最近の事例を以下に示すが、それらは過去に見られた「保険統計的」慣行というよりも、より特化した収集徴候を示唆している。

４.２　中国政府が指示した「専門的」スパイ行為

中国の専門的インテリジェンス機関のためにスパイ活動を行っているエージェントは、上記に述べたより自由な「保険統計的」収集手法とは対照的に、より特化した種類の技術とインテリジェンス情報を捜し求めている。ここ数年間に公にされた中国関与が顕著なスパイ行為事件 3 件は、このパターンを示している。そこでは、収集家が中国政府に代わって活動し、上位当局者が課した特定の技術又は情報要求事項を追い求めている。

４.２.１　Chi Mak 事件

Chi Mak は、スパイ行為捜査対象者の中心人物であった。彼の活動は 2005 年 10 月の逮捕によって最後を飾り、2008 年 3 月に 24 年間の禁固刑判決が宣告された。Mak 氏は、中国の広州省に生まれ、1980 年代の初期に南カリフォルニアに移住し、1985 年に帰化して合衆国市民となった。彼は 1996 年まで、カリフォルニアのアナハイムにある Power Paragon 社のエンジニアとして勤務していた。この Power Paragon 社は L-3/SPD Technologies/Power Systems Group の子会社であり、彼には「Secret」レベルの秘密保護適格証明書が付与されていた。逮捕時の Mak 氏は、将来合衆国海軍戦艦用の「Quiet Electronic Propulsion(低雑音電気推進装置)」プロジェクトの主幹プロジェクト・エンジニアとして勤務していた。

Mak 氏は、Power Paragon 社の他のプロジェクト関連情報は無論のこと、この低雑音電気推進装置プロジェクト関連の情報を入手の上自宅に持ち帰り、コンパクト・ディスクに情報をコピーした後、彼の兄弟 Tai Mak に同ディスクを渡して暗号化を依頼した。Tai Mak は、Chi Mak の運び屋として活動し、中国広州省の身元不明の中国担当者に同資料を中継ぎする役割を担っていた。Tai Mak は 2005 年 10 月末、低雑音電気推進装置とその他のプロジェクト関連のデータが記憶されているディスク一式を、この広州省の身元不明の人物に配達するつもりであったが、その旅程中のロサンゼルス国際空港において FBI 捜査員に逮捕された。

FBI 捜査員は Chi Mak と Tai Mak の逮捕に先立ち、Chi Mak の自宅ゴミ箱から切り刻まれた文書を回収した。それには、Chi Mak に対する中国のハンドラーからの収集指示任務が記されていた。これらの Chi Mak に対する指示には、専門的なつき合いとカンファレンスを通じて情報ネットワークをより拡大することが含まれていた。また、回収された文書には、海軍と宇宙に重点を置いた 18 種類の異なる軍事技術のリストが提示されてい

た。Chi Mak は、これらについてさらなる情報を探し出すことが求められていたのである。

Chi Mak は 2007 年 5 月、カリフォルニア中央地区合衆国地方裁判所において、共謀罪、2 件の輸出規制法違反の企て訴因、外国政府のエージェントとしての登録怠慢、及び連邦捜査官に対する虚偽供述書により有罪の宣告を受けた。彼に対して 2008 年 5 月、24 年間の禁固刑判決が下された。連邦当局の声明は、Chi Mak が叙々に合衆国防衛企業複合体に入り込み、中国政府に代わって軍事技術を盗むため、20 年以上も前に合衆国への移住が許可されていたことを指摘した。

この Chi Mak 事件は、中国の軍事研究開発セクターが開発中の特定合衆国軍事技術に強い関心を抱き、それらに密かにアクセスしようとしている側面を如実に示すものである。Chi Mak によって危殆化された情報は、中国の海軍システム近代化プログラムに相当な利益をもたらすとともに、現在開発中の合衆国システムのぜい弱性を明らかにする中国エンジニア能力の向上に寄与することになるであろう。(さらなる詳細については、本報告書第 2 章第 2 節「中国海軍の近代化と戦略」を参照されたい)

４.２.２　Bergersen と Fondren 事件

2008 年～2009 年の互いに関連する 2 件の中国スパイ事件は、ハイブリッド型の素人-専門家のスパイ行為モデルとしての側面を見せている。これらの事件では、外見上素人のエージェントすなわち情報提供者と見られる人物が、合衆国政府職員から秘密区分指定及び部外秘の情報を盗み出すよう中国政府から指示を受けたのである。その最初の事件は、2008 年 2 月に 3 人の逮捕者が出て衆目を集めることとなった。3 人は、台湾生まれの帰化合衆国市民 Tai Shen Kuo、正規の合衆国在留外国人中国市民で Kuo の助手として働いた Yu Xin Kang 及び FMS(Foreign Military Sales)を実施する国防総省一機関の国防協力機関(Defense Security Cooperation Agency)の兵器システム政策分析家 Greg William Bergersen である。

Tai Shen Kuo は、ニューオーリンズで家具ビジネスを営むとともに、家族の縁故を通じて台湾の国防担当者と密接な接触関係を維持していた[160]。彼は、公開されていないものの一連の出来事により、中国広州の中国高官と友好関係を結ぶようになった。宣誓供述書には、この中国高官の氏名は明らかにされていない。この人物は、Kuo 氏に資金を提供するとともに特定品目の情報を指定して、合衆国政府内の彼の連絡相手から同資料を入手するよう命じた。

Kuo 氏は、彼が台湾の縁故を利用して有利な将来防衛契約取引の基礎を築きつつあり、彼のビジネス展開準備を促進するため、台湾の軍事システムや将来の兵器売却に関連する情報を求めているとして、Bergersen 氏をだました。Kuo 氏は、現金と贈り物で Bergersen

---

[160] Tai Shen Kuo は、元中国共和国海軍総督で第二次世界大戦と 1945 年～1949 年の中国市民戦争において国民党の軍務に就いた Hsueh Yeh の義理の息子である。詳細については、Peter Enav 著、「台湾が最近の合衆国スパイ告訴の影響を再考」、台湾タイムズ、2008 年 2 月 14 日を参照、次により入手可：http://www.taipeitimes.com/News/taiwan/archives/2008/02/14/2003401185.

氏にしつこく迫り、期待される将来の軍事契約取引のビジネス・パートナーになれるとの希望を抱かせ、彼をだましたのである。Kuo 氏は、Bergersen 氏から「広大な勝利プロジェクト(Broad Victory Project)」に係る情報を入手した。これらの情報には、台湾の軍隊が合衆国の援助で開発した指揮統制システムの向上プログラム、国防総省の通信ネットワーク「グローバル情報グリッド」に係る出版物、及び(秘密区分指定が『Secret』の)「Javits 報告」からのデータが含まれていた。Javits 報告からのデータは、今後 5 年間に及ぶ合衆国の外国に対する軍事装備品売却計画に係る国防協力機関の 2007 年版スプレッドシートであった。

Bergersen 氏は、グローバル情報グリッドや台湾に対する将来の軍事装備品売却係る情報など、少なくともいくつかの場合において Kuo 氏からの具体的な要求に応えていた。Kuo 氏は、元を正せば広州の氏名不詳の中国高官の指示を中継ぎしただけなのである。Bergersen 氏は、Kuo 氏に文書や情報を手渡していた間を通じ、それらの情報が中国ではなく台湾の高官に向けられているらしいと信じていた。したがって、彼は古典的な「false flag」作戦（偽装作戦）にだまされたのである。False flag は、情報のエンド・ユーザーのアイデンティティに関して誤った情報が伝えられる、というものである。

Tai Shen Kuo に利用されたその他の情報源は、ペンタゴン内の合衆国太平洋軍ワシントン連絡室の副長として 2001 年 8 月から 2008 年 2 月の間勤務していた合衆国空軍退役大佐の James Fondren であった。同大佐と Kuo 氏の結びつきは、少なくとも 1998 年にさかのぼる。それは、伝えられるところによれば、Fondren 氏が自宅で営んでいたコンサルティング・サービス「Strategy, Incorporated(有限会社戦略)」の唯一の顧客に Kuo 氏がなった時とされている。Kuo 氏は、2008 年 2 月の Kuo 氏逮捕時、実際に Fondren 氏の自宅に客人として滞在していた。

Kuo 氏は、Fondren 氏のコンサルティング・サービスを介して、合衆国と中国の軍-軍間の結びつきに係る話題についての「意見書」を Fondren 氏に求めた。これらの意見書の題目には、中国軍高官の合衆国訪問、国防総省と PLA 高官間の防衛論議の概要、及び合衆国海軍と PLA 海軍の合同演習アセスメントが含まれていた。伝えられるところによれば、捜査官による Fondren 氏の「意見書」の精査の結果、秘密区分指定が「Confidential」と「Secret」の文書から抜粋された一節のいくつかが、ほとんどそのまま複写されていたとされている。

また、Fondren 事件の宣誓供述書は、Kuo 氏の中国ハンドラーが、Fondren 氏に伝えるべき関心のある話題を Kuo 氏に与えたこと、及び Fondren 氏が、自身の「意見書」が台湾の軍高官に向けられていると誤解するよう提案したことを指摘している。これが真実であるとするなら、Fondren 氏も Bergersen 氏と同様に、Kuo 氏によって「False flag」の下にだまされたことになる。伝えられるところによれば、Fondren 氏は Kuo 氏のハンドラーとの直接連絡をも維持し、1999 年と 2000 年に同ハンドラーと 40 の E メールを交換したとされている。

Gregg Bergersen と James Fondren の行為は、従来の中国国家後援の合衆国に対するスパイ行為の特徴からは相当シフトしていることが指摘できる。これらの事件と従来の中国モデルとの間には相当な違いがある。それらは、両男性とも、合衆国政府の職員で秘密区分指定情報へのアクセス権を持っていたこと、中国系アメリカ人ではないこと、手渡すべき具体的な文書や情報を課されていたこと、及び情報提供に対する報酬を受け取っていたことである。このことは、一連の慣行がより「古典的な」スパイ行為モデルに近づいていること、中国インテリジェンス諜報員側が、ますます好んで、要求された特定の情報にアクセスすることができる合衆国の人物を探し求めていることを示唆するものである。

Gregg Bergersen は 2008 年 3 月 31 日、ヴァージニア州東部地区合衆国地方裁判所において、国家の安全保障に係る秘密情報を開示したとする 1 件の共同謀議訴因に対して有罪を認める答弁を行なった。そして、2008 年 6 月 11 日に 57 か月の禁固刑の判決が宣告された。Tai Shen Kuo は 2008 年 5 月 13 日、ヴァージニア州東部地区合衆国地方裁判所において、国家の安全保障に係る情報を外国政府に渡したとする 1 件の共同謀議訴因に対して有罪を認める答弁を行なった。そして、2008 年 8 月 8 日に 188 か月の禁固刑と罰金 40,000 ドルの判決が宣告された。James Fondren は 2009 年 9 月 25 日、1 件の外国政府エージェントに対する秘密区分指定情報の不正伝達訴因及び 2 件の FBI に対する虚偽声明訴因により連邦陪審により有罪を宣告された。彼に対しては、2010 年 1 月 22 日に判決が宣告される予定である。

４.３　中国の国家が管理する研究所と民間組織による「組織指示」のスパイ行為

中国の合衆国に対するスパイ行為の相当な部分は、専門的な中国インテリジェンス・エージェントの命令を受けて実施されているようであるが、そのほとんど、とりわけ経済スパイと企業スパイについては、国有の研究所及び中国軍-企業複合体会社やこれらの国家機関から分離新設された子会社によって行われている。CIA 及び FBI が述べているように、「中国の民間組織は、特許権/企業機密の合衆国技術を追求する重要な役割を担っている。合衆国にある中国の民間組織の大部分は、合法的な会社である。しかしながら、そのいくつかはインテリジェンス収集活動のプラットフォームなのである」　多くの個々の収集事件は計画性がなくばらばらに行われているようだが、1980 年代にさかのぼると、技術取得と近代化に係る中央集権的な国家レベルの中国プログラム「863 プログラム[161]」があり、そこでは先進技術を取得するための広範な活動を強調している。

「組織指示」のスパイ行為もその重要性を増しており、無作為でなく、より的を絞った形で実施されていると思われる。国防保全局が 2008 年に出版した非秘密区分指定の報告書は、民間組織によって実施された規制技術に対する標的行為活動の増加に言及しており、これは「目的を持って接触を企てる場合、関心を抱いている政府又は政府関係組織に代わって非政府組織を利用した方が、より当たり障りのないように思われる」ことを断言して

[161] 訳注：1986 年 3 月に発表された中国の技術高度化計画をいう。

いるものと思われる。国防保全局の報告書は特定の国を示していないが、同報告書内において、合衆国防衛技術を不正に取得する活動の発生源として最も多いのは、東アジア太平洋地域であると断言している。

とはいえ、仮に国家が関与する民間及び研究組織による特定技術を攻撃目標にした組織的協調活動がますます増加しているとしても、それらに対する収集の優先順位や任務遂行プロセスは、これまで十分に文書化又は理解されていなかった。Center for Intelligence Research and Analysis, Defense Group, Inc.の理事である James Mulvenon は、本委員会において、国家の指示と民間の先導的行為の両者が交互に行われている複雑なプロセスであるとし、この件について次のように説明した。

> 私は、これはボトムアップとトップダウン両者からのプロセスであると思う。・・・・我々は、「科学と技術」調達に関して高いレベルの国家調整があり、それは中国の情報産業部[162]の下で調整されるのか、科学技術部内で調整されるのか又は 863 プログラムから派生したものかのいずれにせよ、北京レベルに及ぶものであることをオープン・ソースから認識している。この 863 プログラムは、それ自体が高レベルの国家調整がなされたものであり、中国が推進すべき主要技術のギャップを明示している。・・・・同時に、ボトム・レベルにおいて革新が進められている。そこでは、人々が自身の物質主義利益に基づいて価値があると思う物の取得を企て、その顧客を探している。・・・・したがって、私は、ボトムアップとトップダウンの両プロセスが同時に作用していると考える。

Mulvenon 博士は「組織駆動(enterprise driven)」収集の根拠についてさらに詳しく述べ、1990 年代末の防衛改革の過程において中国政府管理の防衛企業研究所から分離新設された利益追求型の民間会社は、技術取得に関して突出した役割を担っていると説明している。また、彼は技術取得追及のための分散化されたフリーマーケット・システムについても、次のように説明している。

> それは、単にファックスに書かれている事を読む程度のありきたりなものです。そこには、我々が興味を抱く品物の買い物リストがあります。彼らがどこでそれらを捜し求めるのかついて、明確な案内はありません。彼らが接触した人物の請負人としての適任性と積極性に委ねるだけなのです。・・・・請負人は、ネットワーク内の人物に限らないのが一般的です。これは冗長性のある複数任務が付与されている分散ネットワークなのです。「そこに誰が最初に行き着くかが問題」なのです。

---

162 英語では Ministry of Industry and Information となっている。我が国で考えると中華人民共和国政府(中国)の「省」ということになるが、中国では「部」としている。

４.３.１　Dongfan「Greg」Chung 事件

最近公表された「組織指示」による企業スパイの一例は、中国生まれの合衆国帰化市民 Dongfan「Greg」Chung 事件である。Chung 氏は 1973 年～2006 年の間、合衆国の航空機産業で働いており、ボーイングとロックウェル・インターナショナル両社に勤務していた。彼は、「Secret」レベルの秘密保全適格証明書を持ち、様々な航空宇宙プロジェクトのエンジニアとして勤務していた。それらのプロジェクトには、宇宙シャトル胴体のストレス・テスト分析、宇宙シャトル通信用フェーズド・アレー・アンテナの開発などが含まれていた。

Chug 氏は 2008 年 2 月、カリフォルニア州オレンジで逮捕された。彼の事件に対する起訴状によれば、彼は 1979 年ごろ、Harbin Institute of Technology の教授と接触し、「中国の『科学近代化』に貢献してくれないか」と申し出た。さらに、Chug 氏は翌年、中国国家航空機技術輸出入会社、Nan Chang 航空機会社及び中国航空機産業会社の重役と連絡をとり、彼らから航空機開発に係る極めて具体的な質問事項と詳細な技術情報の入手依頼を受けた。Chug 氏はこれに応えて中国で講義を行うため、会社に報告することなく何度か中国に旅行した。また、彼は、ボーイング及びロックウェル社所有の多数の技術マニュアルを、郵便で又はサンフランシスコにある中国領事館のある人物に手渡した。これらの資料の中には、1985 年に発送された機体ストレス分析関連の 27 件の資料及び B-1 爆撃機プログラム関連の 24 件の資料が含まれていた。

Chug 氏は 2009 年 6 月 16 日、カリフォルニア州中央地区合衆国地方裁判所において、経済スパイを犯した共同謀議により有罪を宣告された。その内容は、6 件の外国の利益に供した経済スパイ訴因、1 件の中国エージェントとしての活動訴因、及び 1 件の FBI に対する虚偽声明訴因である。Chug 氏は 2009 年 11 月 9 日に、判決が宣告される予定である。

４.４　中国の代理としての「請負スパイ」

中国のインテリジェンス収集に特有なものとして、これは合衆国のセキュリティの観点からは極めて重大なものでもあるが、民間人が独立に又は中国政府に代わってスパイ行為に及ぶことがある。国家インテリジェンス局は、この件に関し次のように報告している。

> 非専門家によるインテリジェンス収集、これには政府と民間の研究者、学生、学者、科学者、ビジネスマン、代表団、訪問者などが含まれるが、これらも相当量の機微な合衆国技術及び企業機密を中国に提供している。これらのグループ・メンバーの中には、故意又は知らずに、中国インテリジェンス機関又は中国の防衛企業の代理として収集に及んでおり、我が国に対する重大なインテリジェンス脅威となっている。しかし、これら民間セクターの人物による収集活動事例の多くは、全く商用利益又は専門的知識を得る機会に駆り立てられたものであって、中国インテリジェンスとの協力関係はない。

このような素人の活動に依存した科学技術情報の収集は、中国人の学生、貿易代表団、ビジネスマン、教育研究機関などによる、おびただしい数に及ぶ「請負の」経済スパイと企業スパイへ結び付けている。このような民間人によるスパイ行為の動機の範囲は、多様であり、複雑である。元 FBI 特別捜査員の I.C. Smith は、国家安全部は教育又はビジネス目的で海外に行く中国市民に圧力をかけ、海外旅行許可の対価として外国の技術情報を求めることがある、と証言している。しかしながら、この「請負スパイ行為」の現象は、とりわけ中国の会社と直接の結びつきを持つ者や中国に合衆国の管理下にある技術を輸出しようとして合衆国の輸出管理や経済スパイ法の回避を追求するビジネスマンにとって、一般的なものとなっている。このような場合、利益が主たる動機となる。もっとも、多くの事例において、「中国を助けたい」とする動機は、個人による金銭取得期待の動機と交差するものである。

このように個人的に計画され実行されたスパイ活動は、多くのやっかいな問題を合衆国カウンターインテリジェンスと法の執行当局に引き起こしている。元 FBI 特別捜査員の Smith は、「インテリジェンス機関が存在しないのは、本当にインテリジェンス活動といえるのか？」と疑問視している。とはいえ、国家の直接関与がない場合でも、企業スパイで取得された技術によって主たる恩恵を被るのは中国政府なのである。

「請負スパイ行為」は、最新のハイテク・データや装置を取得することに必ずしも焦点を当てているものではない。Mulvenon 博士は、多くの古い技術であっても中国軍の近代化にとっては価値があると考えられるとして、本委員会で次のように証言した。

> 私は、我々の輸出管理システムが最新の技術に対して過度の焦点を当てており、中国が特定の技術情報の欠片(かけら)を求める理由についての手段 - 目的テスト(means-ends test)を行っていない、ということに関しても委員会に提議したい。ここに中国が取得しようとしている技術情報の欠片(かけら)がありますが、それらは 20～25 年前の古い技術です。そして、それらは既存の合衆国防衛システムの大黒柱となっているものであり、最新技術とは程遠いものと考えられるものです。とはいえ、手段－目標テストを行うことによって、それらの技術情報を中国システムの重要なギャップとして正しく識別することができると思われます。

Mulvenon 博士は、この点についてさらに説明を加え、多くの請負「零細」企業が存在し、それらの多くは居住住所における名義だけのビジネス登録以外の何ものでもないが、合衆国の製造会社若しくは防衛企業設備品オークションの流通市場から又はインターネットからでさえも古い軍事技術を合法的に取得した上で、中国での顧客を探していると本委員会で述べた。

４.４.１　中国の宇宙産業に利益をもたらした２件の産業スパイ事件

本委員会による 2009 年報告書の作成期間において、説明に役立つ産業スパイ 2 件が合衆国内で発生した。これら両者とも、中国の宇宙産業の急速な進展の助けとなる合衆国管理下の技術と資料の中国への不正輸出を企てたことに関するものである。以下に述べる事件は、航空宇宙関連技術の狭い分野に限定しているものの、包括的なリストとは程遠いものでる。他の事件については、米中経済安全保障調査委員会 2009 報告を参照されたい。

第一の事件は、ヴァージニア州ニューポート・ニュースにある AMAC International Inc. 所有者 Quan-Sheng Shu に係るものである。Shu 博士は 1940 年上海で生まれ、1998 年に合衆国市民として帰化した。彼は、物理学の博士号を持ち、低温学と超伝導のテーマに関連する 6 冊の本と 100 件以上の論文を執筆した。Shu 博士と彼の会社は、合衆国エネルギー省と米航空宇宙局に代わっていくつかの研究開発契約に係る仕事に取り組んだ。

Shu 博士は 2008 年 11 月に、ヴァージニア州東部地区合衆国地方裁判所において、2 件の武器輸出管理法違反訴因と 1 件の中国高官に対する贈賄に伴う対外贈収賄法違反訴因に対し、有罪を認める答弁を行った。Shu 博士は、51 か月の禁固刑と罰金 386,740 ドルの刑に処せられた。AMAC International は 2009 年夏の時点で、過去の多くのプロジェクトと知的所有権に係る技術を放棄するとともに、北京にあるオフィスを閉鎖した。

Shu 博士の輸出管理法違反内容は、宇宙打ち上げ飛翔体用の低温給油システム及び液体水素タンクと低温装置用の技術データを中国へ輸出したことであった。Shu 博士が輸出した品目は、中国海南省南部の島にある重搭載量打ち上げ施設で利用される予定の宇宙打ち上げ飛翔体用低温給油システムであった。司法省によれば、海南の宇宙打ち上げ施設は、PLA と中国飛翔体打ち上げ技術院との密接な連携の下に、宇宙ステーションと人工衛星、有人宇宙飛行及び将来の月ミッション用の打ち上げサイトとして予定されている。

第二の事件は、中国の宇宙プログラムを支援したことに対する輸出違反の容疑であり、ミネソタ州の合衆国地方裁判所大陪審が 2008 年 10 月 28 日に、Jian Wei Ding、Kot Tong Lim と Ping Cheng の 3 名を起訴したことにより明らかにされた。Jian Wei Ding と Kot Tong Lim は、両者ともシンガポールにある輸出入会社 FirmSpace Limited の役員であり、Ping Cheng はニューヨーク在住者であって、伝えられるところによれば FirmSpace 全株主であるとされている。伝えられるところによれば、この 3 名は、航空機、ロケット、宇宙飛行体及びウラニュウム濃縮に適用されるカーボン・ファイバー資材の中国宇宙技術院への売却計画に関与していたとされている。伝えられるところによれば、Ding 氏と Lim 氏は、遠隔操作電信送金を介してミネソタ州にある未公開会社からカーボン・ファイバー資材を調達し、ニューヨークの Cheng 氏の住所に出荷した。伝えられるところによれば、Cheng 氏は、それらを点検の上保管し、中国宇宙技術院宛ての出荷準備をした。この他の人物 2 人、FirmSpace 社の部長 Hou Xinlu と Gao Xiang は、この事件に関連して名前が

挙げられたが、罪を免れた。両者とも中国に居住していると信じられている。

シンガポールの地方メディアは、FirmSpace 有限会社がビジネス活動の点で何もしていなかったようだと短評した。ある地方ニュース放送局は、会社に注目すべきビジネス活動が欠如しているにもかかわらず、会社が従業員を一時解雇もしないできちんと給料を支払い続けていた、と言及した。会社の受付係からの次のような言葉が引用されている。「私は本当におかしいなと思ったのです。でも、私は給与をきちんといただいていたので、ボスに訊ねようとは思いませんでした」

５　この情報がどのように上手く処理されたか？

中国のシステムは、このような膨大なデータや資料を取り込んで、大量のもみ殻から有用な情報の小麦を実際どのように効果的に分離しているのであろうか、という疑問が残る。中国政府のお役所仕事の特徴は、担当者がキャリアアップの目的で上位者に対し成功を誇張する傾向にあり、このことがシステムの浪費性を促進している。例えば、元 FBI エージェントの I.C. Smith は、合衆国内の軍事技術を取得する個人の責任について元国家安全部の将校とインタビューした際、同将校が合衆国軍の役に立たない余剰品目の収集に浪費した時間は単に官僚的見せかけに過ぎないと彼に語った、と述べている。

しかしながら、中国のシステムによって収集された膨大な量の装置や情報の中に、価値ある真に有用な資料が現れることがある。1990 年代末のある報告書は、実際に PLA 関連組織が合衆国軍事基地からの余剰放出物品購入に関与したとしており、このような方法でリバース・エンジニアリングに必要な合衆国軍事システム・モデルを取得することができたと思われる。余剰放出物品の中には、パーシングⅡ中距離弾道弾ミサイル・システム用のレーダー・デジタル誘導システムが含まれていた可能性がある。

６　海外の反体制派中国人グループに対する標的行為

合衆国内の中国インテリジェンス活動におけるその他の極めて重大な側面に、そして合衆国の多くの市民や外国人居住者に対する妨害効果をもたらすものに、中国政府諜報員による海外で活動している反体制派中国人への徹底的な監視、嫌がらせ及び分離工作活動の徹底的な促進がある。合衆国内の中国当局者によるこのような活動については、多年にさかのぼり、有り余るほど十分な証拠がある。元中国領事の職員で合衆国に亡命を求めた Lin Xu は 1990 年 6 月、下院外務委員会における宣誓証言において、天安門広場虐殺の直後に国家安全部の高官がワシントン DC の中国大使館を訪問し、教育部門担当の領事職員と相談した、と証言した。その後これらの職員に、改革論者又は民主主義擁護者と思われた合衆国内の中国人学生に対する監視と嫌がらせの任務が付与された。

また、ここ数年、全く同じような、そしてより詳細な報告が中国亡命者から寄せられている。元中国主席事務官でオーストラリアのシドニーの領事であった Chen Yonglin は 2005 年 5 月、中国から離反しオーストラリアに亡命を求めた。Chen 氏は、中国政府当局

による「敵対性要素」に対する監視、嫌がらせ及び妨害活動に関し、具体的で詳細な報告書を提供した。Chen 氏は、同じモデルの中国インテリジェンス活動がオーストラリアと合衆国両国に適用されていると明言した。

Chen 氏は、法輪功メンバー、チベット人分離独立派、ウィグル人分離独立派、台湾独立活動派及び民主主義擁護者からなる「5 つの有害グループ」に言及した中国政府内部文書を作成した。さらに同文書は、このようなグループに対する「戦闘における領事館の主たる迎撃戦略」として、領事館の職員に対し、リストに氏名が掲げられた活動家の「監視強化」を実施すること、特に地方の中国語メディアに焦点を当て、複数のチャネルを介して宣伝活動を実施すること、及び「地方自治体当局者に働きかける」ことを指示している。Chen 氏は、後者の活動について具体的な活動を述べている。すなわち、オーストラリア当局に対し経済的圧力の代償を賦課すること、及びシドニー地域の教育当局が、校長が法輪功メンバーであった学校への公債を拒否するよう議員に働きかけることである。中国政府当局者によるこのような強化活動の中核は、中国利益の代理として活動する「地元の中国人社会の動員」である。

合衆国における法輪功活動家は、Chen Yonglin が述べたのと本質的に同様の活動を中国領事職員が行っていると主張している。法輪功関連の新聞である Epoc Times は、中国ニューヨーク領事館の職員が 2008 年に、ニューヨーク市クィーンズ区フラッシングのニューヨーク街区の法輪功デモ参加者に対して、一連の猛攻撃を計画したと断言した。

本年、本委員会の場で語った専門家の参考人 2 人は、どちらも法輪功と何らの関係もない人物であるが、中国大使館と領事館の職員が中国系アメリカ市民を組織化して動員し、中国政府に代わって行動させるための積極的な役割を果たしている、と証言した。

中国領事館職員による最近のその他の華僑グループ動員例としては、2008 年春の世界中を走るオリンピック聖火リレーの間に見られた。聖火リレーが北京に近づくにつれ、いくつかの都市において、チベット支持者、人権擁護者、その他の中国政府に批判的な活動家と、中国人学生又は地元の華僑居住者から構成されたデモ隊反対者との間に取っ組み合いが発生した。これらの都市のいくつかにおいて、とりわけパリとソウルでは、これらの対立が暴力沙汰になった。

合衆国内におけるこのような一例は 2008 年 4 月 8 日に、ノース・カロライナ州ダーラムのデューク大学構内における抗議と、抗議に対する大反論の場で発生した。このインシデントは、一人の中国人女子学生による 2 つの敵対するグループ間の調停の企てが、インターネット上で国家主義活動家に中傷され、そして彼女の両親が住む中国の家がこれに続いて破壊された後、かなりの数のメディアの注目を引いた。デューク大学のインシデントでは、約 15 名の大学人権グループの学生が聖火リレーの日に合わせてチベット支持集会を計画した。しかし、彼らは、約 400 名の反デモ隊に囲まれ、引きずり出されてしまったのであった。以上は、このインシデントを目撃したデューク大の学生が本委員会に提供した具体的で詳細な報告書によるものである。

多くの事例において、中国大使館又は領事館職員によって抗議者に反感を持つ華僑グループが奨励され組織化された、とする明確なサインが示されている。分析会社 Strategic Forecasiting Inc.が 2008 年 4 月 9 日のサンフランシスコ市内を貫く聖火リレーの通過に関して提出した報告書には、次の記述がある。

> 中国支持のデモ隊は 4 月 9 日午前 8 時までに、食べ物と飲料水、及び中国、合衆国とオリンピックの旗を持ち、計画された聖火リレー・コースに沿って道路の片側に並んで場所を占領した。しかしながら、これらは、北京のメディアが描写したような祖国を支持する海外中国人による自然発生的な集合ではない。むしろ、そこには地元の中国人のビジネス・社交団体と領事館との間に調整された活動があって、大きな中国支持者の集まりを呼び寄せ、準備し、展開し、組織したものである。ある見積もりによれば、中国人で満席の 50 台のバスがカリフォルニアの他の場所からサンフランシスコに集結したとされている。

また、この報告書は、反中国デモ参加者の携帯電話に対するいたずら電話、テキスト・メッセージ、さらには低レベルの局所的なジャミングの利用についても主張している。これが真実であるとするなら、中国に対して抗議を計画する活動家の電話番号が予め知られていたことを証拠付けるものとなる。同報告書には、反中国デモ参加者が暴力的に思えるようにするため、次に示すような争いを起こさせる活動の可能性についても記述されている。

> 多くの場面において、カメラを持った個人又は小グループの人物が、反中国デモ参加者による衝突や暴力的行為を探し求めていたと思われる。彼らは、大きな中国国旗を持って、チベット解放又はダルフール救済デモ参加者の中央部分を頻繁に歩きまわったり、反中国デモ参加者の中を前後に行き来たりした。そして、いくつかの場面において小競り合いが突発し、スナップ写真が撮られた。もっとも、反中国デモ参加者はすぐに気付いて、敵対する両者を切り離そうとした。中国のメディアは同じ日に、チベット支持デモ参加者が親中国デモ参加者を後方から乱暴に押しやる場面の写真を掲載した。これは、中国メディアの要点がチベット支持者は暴力的であると「証明」することにあるからである。

中国系アメリカ人の動員又は監視のいずれかにかわるがわる努力を向けるこのような活動は、どこの華僑でも本質的には北京に忠誠を尽くすものだとする中国当局者に浸透した姿勢によって、ある程度説明することができる。

このような例は、中国政府が海外で計画される反体制派又は少数民族活動を極度に恐れるとともに、これらの主張を支援する活動家グループの目的達成を妨害するためには、相

当な注意と資源を充てるのをいとわない、とした姿勢をあざやかに描写するものである。これらはまた、中国政府当局者が、彼らの代わりに活動を請け負う地元華僑のビジネスやコミュニティ・グループを仲間に加えたり動員したりすることによって彼らのやり口を隠そうとしたとする、Chen Yonglin の報告書内容をより説得力あるものとしている。この活動パターンは、中国共産党(CCP)が中国政府の支援を得てその政治的責務として国内の視聴者に世界中の中国人の談話を提供する文脈の中で考えると、最もよく理解できる。また、これは、非共産党中国人グループを打倒し、中国共産党の目標到達を促進させるためのツールにするとした、長年の「統一戦線」中国共産党活動にも適合するものである。

7　結論

- ✧　中国政府のインテリジェンス機関は、合衆国と合衆国の利益を攻撃目標とした活動に積極的に関与している。中国は、合衆国に対するスパイ行為を最も積極的に行っている国である。そして、その活動の中心を中国軍の近代化と経済力発展に有益な合衆国情報と技術の取得に置いている。
- ✧　中国に代わって行われたスパイ行為の中には、ノンプロ収集家によって実施されたものもある。これらのノンプロ収集家の動機付けは、利益、愛国心、民族的血族関係又は強要である。たとえ、多くの窃盗や管理下にある技術の違法輸出事件において、国家の直接関与が不明確であったとしても、中国政府はこのような活動を奨励し、それらからの利益を得ている。
- ✧　中国が関与した最近のスパイ事件は、中国系アメリカ人コミュニティ外の情報源を利用した情報収集活動に、その焦点を当てているとする証拠を示している。
- ✧　中国の諜報員と領事館職員は、合衆国本土の中国反体制派グループに対する監視と嫌がらせを積極的に行っている。

第４節　合衆国を攻撃目標とした中国のサイバー活動と合衆国国家安全保障に及ぼす影響

１　序論

オバマ大統領は 2009 年 5 月、サイバー攻撃を国家が直面する「最も重大な経済及び安全保障上の難問」であるとした。前国家カウンターインテリジェンス行政局長官 Joel Brenner は、中国が合衆国を攻撃目標にした大規模な悪意のあるサイバー活動の発生源であると認定した。間接的な証拠は、中国の合衆国政府及び防衛関連の情報を標的とした攻撃が損害を与えていることを示唆している。例えば国防総省内局は 2007 年 7 月、調査官が中国に起因するとした重大な侵入に対する防衛処置として、1 週間以上も情報システムをオフラインにした。2009 年 4 月の報道は、防衛関連企業の情報システムが 2007 年と 2008 年に、おそらく中国から活動していると思われる侵入者により、合衆国の最先進戦闘機の一つである F35 ライトニングⅡの「設計及び電子システムに係る数テラバイトのデータ」を首尾よく持ち出されたとことを明るみにした。多くの状況及びフォレンジックの両証拠は、国家組織による直接活動又は国家が後援する第三者の活動のどちらを介するにせよ、このような活動に対する中国国家の関与を強く指摘している。

悪意のあるサイバー活動は、重要インフラを破壊、商取引と銀行取引システムを混乱、及び機微な防衛と軍事データを危殆化させる可能性を持っている。悪意のあるサイバー・インシデントが高進しつつあり、かつ、合衆国政府コンピュータ・システムが攻撃されていることは、この問題の重要性を明らかにするものである。当時合衆国戦略軍グローバル・ネットワーク・オペレーション・ジョイント・タスク・フォースの先任幕僚であった Gary McAlum 大佐は 2008 年 5 月、本委員会における証言において、国防総省に対する悪意のあるサイバー活動件数が 2007 年に 43,880 にも及んだと明言した。この数値は 2008 年に、約 20%増加し 54,640 に達した。2009 年前半の数値は、本年も同様に急激な増加となることを示しており、1 月 1 日～6 月 30 日の間で 43,785 に上るインシデントが発生した。この傾向が 2009 年末まで続くとすれば、悪意のあるサイバー活動は 2008 年に比べ 60%増となる。このような攻撃に伴うコストは相当なものである。グローバル・ネットワーク・オペレーション・ジョイント・タスク・フォース副司令官 John Davis 陸軍准将は 2009 年 4 月、ちょうど 6 か月前に、合衆国陸軍が陸軍のネットワーク攻撃に対する修復に要したマンパワー、時間、契約者、ツール、技術及び手順に係るコストは、1 億ドル以上にも上ったことを明らかにした。

合衆国政府行政部は 2009 年、国家の安全保障に対するサイバー脅威に取り組むため、いくつかの対策を講じた。ホワイトハウスは 4 月、合衆国政府の諸機関の間のサイバーセキュリティ・プロセスに対するより中央集権化された「トップ・ダウン」アプローチを管理するとともに、国家のサイバー政策と標準について勧告を行う「サイバー・セキュリティ調整官(Cyber Security Coordinator)」(通称、「サイバー独裁者(Cyber Czar)」)と呼称さ

れるポストの創設を発表した。同調整官は、行政管理予算局を介して新及び既存のイニシアティブ(構想、推進計画、プロジェクトなど)に対する予算管理を行うとともに、国家安全保障会議及び国家経済会議の両者に対し報告を行うとされている。国防長官 Robert Gate は 2009 年 6 月、「国防総省のサイバースペース作戦に対する包括的アプローチを展開」するため、国防総省に対し統合サイバー司令部の編成を命じた。同サイバー司令部は、国家安全保障局を含めるとともに、少なくとも当初は合衆国戦略軍の下位組織に位置付けられ、伝えられるところによれば、国防総省の攻撃的及び防衛的サイバー能力を統合するとされている。このサイバー司令部が、非防衛、すなわちインテリジェンス関連政府ネットワークと民間のネットワーク・インフラをセキュアなものとするため、どの程度の活動をするかは不明確なままである。これらに係る責任の大部分は、国土安全保障省が引き継ぐことになると思われる。

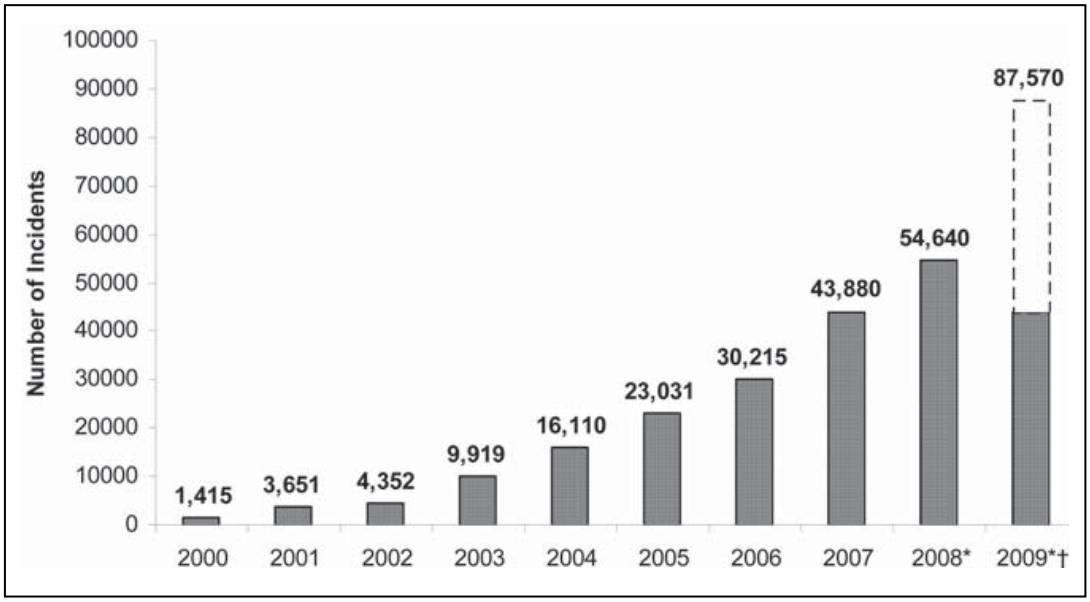


図 1：国防総省が報告した悪意のあるサイバー活動インシデント数(2000–2008。2009 年は予測値)

出典：米中経済安全保障調査委員会、中国の拡大戦略とサイバー・宇宙戦能力の開発、Garry MacLum、2008 年 5 月 20 日。

＊出典：匿名（合衆国戦略軍幕僚)、委員会スタッフによる電話インタビュー、2009 年 8 月 28 日。

＋：塗りつぶされた棒グラフの数値は、合衆国戦略軍が提供した 2009 年 1 月 1 日～6 月 30 日に報告された悪意のあるインシデント示す。点線で示した棒グラフの数値は、一年中を通して一定の率で攻撃が増加すると仮定したものであり、2009 年 1 月 1 日～12 月 31 日における悪意のあるインシデント数の見積もりを示している。

２　サイバー攻撃責任の所在

中国から発生するサイバー攻撃の分類は容易ではない。ある悪意のある攻撃は民間のハッキング・グループから行われたように見えるが、他の攻撃は国家が後援していることがほぼ確実である。本節が主として焦点を当てる後者は、2 つの重要な要素によってある程度確認することができる。

第一は、 サイバー・インシデントが固有の特徴を置き忘れることから、フォレンジック分析により、時には責任を持つ攻撃者の所属を相当な確かさで明らかにできることである。また、時には調査者が、中国政府の直接関与や人民解放軍(People's Liberation Army: PLA)などの中国政府の具体的な組織を明らかにすることもできる。本節の記述は、サイバー侵入のフォレンジック分析実施に関与した調査者の結論を利用したものであって、利用された技術の完全な説明について公表するものではない。

第二は、攻撃目標となった情報の種類を含め、悪意のある活動の特徴が攻撃者とその所属を推論するに当たっての補完的な情報をもたらすことである。特定の政府及び防衛ネットワークへの標的行為に基づくいくつかの例では、国家の関与を推論することができる。本委員会に提出されたノースロップ・グラマン社の調査によれば、合衆国に対する多数の悪意のあるサイバー攻撃に中国政府が関与していることを示している。

> 中国は、その成熟したコンピュータ・ネットワーク・エクスプロイテーション(Computer Network Exploitation: CNE)能力を利用し、長期にわたって洗練された CNE 攻撃を行い、合衆国の政府と企業に対するインテリジェンス収集の支援活動を行なっているようである。・・・・中国の CNE 攻撃目標が防衛用エンジニアリング・データ、合衆国軍事作戦情報や中国関連政策情報に極端に集中していること、及びその活動範囲が合衆国や世界中の多くの国々を相手にしていることを考えると、このような CNE 活動を支える資源はサイバー犯罪組織の能力や輪郭をはるかに超えるものであり、少なくともある種の国家的支援関係がないと困難である。・・・・持ち出すために攻撃目標とされた情報の種類は、サイバー犯罪におけるクレジット・カード番号や銀行口座情報などと異なり、本質的に金銭的価値がないものである。

グラマン社の調査結果は、攻撃者が中国政府に雇用された者であろうと又は単に情報を売るために盗んだ者であろうと、次のように示唆している。「仮に、盗まれた情報が第三者によりその情報に関心を持つ国々に仲介された場合、その活動は、キーボード操作を実際に行ったオペレータの所属がどうあれ、技術的には『国家の後援を得た』ものであると解釈される」

国防総省のサイバー・セキュリティの定義

本節においては、サイバー活動に利用される戦術を説明する際、次の定義を利用する。

- ✧ コンピュータ・ネットワーク作戦：コンピュータ・ネットワーク攻撃、コンピュータ・ネットワーク防衛及びコンピュータ・ネットワーク・エクスプロイテーションから構成される。
- ✧ コンピュータ・ネットワーク・エクスプロイテーション：コンピュータ・ネットワークを利用し、攻撃目標又は敵対性の自動情報システム又はネットワークからデータを集めることによって実施されるインテリジェンス収集活動をいう。
- ✧ コンピュータ・ネットワーク攻撃：コンピュータ・ネットワークを利用し、コンピュータとコンピュータ・ネットワーク内の情報又はコンピュータとネットワークそれ自身を混乱、妨害、機能低下又は破壊するための活動をいう。
- ✧ コンピュータ・ネットワーク防衛：国防総省情報システム及びコンピュータ・ネットワーク内において、認可されていない活動を防止、監視、分析、検知及び対応を行うための活動をいう。

３　中国のコンピュータ・ネットワーク作戦ドクトリン新事実

中国の国家的活動家の関与を分析することは、中国政府のコンピュータ・ネットワーク作戦分野における透明性が欠如していることから、非秘密区分指定レベルの調査で実施することが困難である。しかしながら、中国政府が後援するコンピュータ・ネットワーク戦プログラムの相変わらずの不透明性はともかく、中国の軍事新聞や軍事専門定期刊行物は、合衆国の1999年のコソボ軍事行動や2003年のイラク侵略などの紛争の際のネットワーク戦と電子戦の能力について以前から賞賛を表明し、中国としても遅れを取り戻す必要性があることを論じている。これらの定期刊行物は、意外にもコンピュータ・ネットワーク作戦に対するさらなる能力開発の必要性について率直な論議を展開するとともに、これらの能力形態のあり方に係る多くの詳細事項さえも提供している。

中国政府はこれまで、国防総省が 2006 年に公開した「統合参謀本部出版物 3-13：情報作戦」に含まれているコンピュータ・ネットワーク作戦などのような戦略又は指導的構想を公開していない。とはいえ、西側の果断な性格のオープン・ソース研究者の中には、これらの定期刊行物に掲載されている議論内容を厳密に調べることで、中国のサイバー能力に係る制度上の新事実を見抜くことができた者もいる。

中国のコンピュータ・ネットワーク作戦関連用語

海軍分析センターの研究者は、中国の軍事執筆者がドクトリン上で用いている主要な用語を明らかにし、それらを次のように翻訳した。

- ✧　コンピュータ・ネットワーク戦：合衆国のドクトリン上の用語「コンピュータ・ネットワーク作戦」の意義に相当する。
- ✧　コンピュータ・ネットワーク攻撃：合衆国のドクトリン上の用語「コンピュータ・ネットワーク攻撃」に同じである。
- ✧　コンピュータ・ネットワーク防衛：合衆国のドクトリン上の用語「コンピュータ・ネットワーク防衛」に同じである。
- ✧　コンピュータ・ネットワーク偵察：合衆国のドクトリン上の用語「コンピュータ・ネットワーク・エクスプロイテーション」の意義に相当する。

本節の中国に関連する文脈の中で上述の用語が使われる場合、それらは合衆国の対応用語と互換性あるものとして利用することとする。

カンサス州フォート・レヴェンワースにある外国軍事研究所の研究者 Timothy Thomas 等は、過去 10 年間における人民解放軍(PLA)のネットワーク戦思想に係る詳細な策定履歴をまとめることができた。PLA は、コンピュータ・ネットワーク戦を現代戦における主要

な作戦遂行手段及びそれ自体が紛争における重要な新領域であるとみなしている。これらの専門定期刊行物の記事は、敵の指揮・統制・コンピュータ・インテリジェンス・捜索及び偵察ノードに対する軍事行動並びに自身のそれらに対する防衛を、現代戦における中心的役割を果たすものとして説明し、そのためのさらなるコンピュータ・ネットワーク作戦の重要性を提起している。また、中国の分析家も、コンピュータ・ネットワーク戦を戦場において弱い軍事戦力で強い敵と互角に戦うための重要なツールとして評価している。

３.１　統合ネットワーク電子戦

また、PLA 当局が出版した文書の分析結果は、「統合ネットワーク電子戦」と題する PLA 運用構想指針の存在を明らかにしている。統合ネットワーク電子戦には、コンピュータ・ネットワーク作戦が従来の電子戦エレメントと協力的な関係で含まれている。

統合ネットワーク電子戦は、コンピュータ・ネットワーク攻撃作戦と従来からのレーダーや通信に対する電子妨害などの電子戦作戦の連携を提唱している。その目標は、紛争の早期段階において敵の指揮・統制・通信・コンピュータ・インテリジェンス・捜索及び偵察システムに対し広範囲にわたる攻撃を行ない、それによって敵対勢力が現代の戦場において勢力を移動し戦うために必要な情報及び通信へのアクセスを妨害することであるとしている。

2009 年の出版物は、統合ネットワーク電子戦に対する骨子を次のように述べている。

> 情報の取得及び伝送を混乱させるための電子妨害、電子欺瞞、電子抑制(周波数帯抑制)などの技法、情報処理及び情報利用を妨害するためのウィルス攻撃又はハッキング、並びに敵の情報プラットフォームと情報設備を破壊するための新たなメカニズムによる対放射線やその他の兵器を利用すること。

統合ネットワーク電子戦のある側面は中国軍の強い願望にとどまっているが、PLA はこの概念を重要視するとともに、サイバースペースを電磁スペクトラムと連携させ、フルスペクトラム現代戦における紛争に不可欠な分野であるとしている（中国の軍事近代化の詳細については、本報告書の第 2 章第 1 節「中国軍と海外安全保障活動」を参照)。PLA の総参謀部が出版した「2007 年の改訂版軍事訓練及び評価の要点」訓練ガイダンスは、PLA の全部隊を対象としたものであり、「複雑な電磁環境下」における訓練を作戦行動と戦術訓練の中核に位置付けている。

このような訓練の最近の例としては、伝えられるところによれば、PLA の陸海空軍約 100 人の高級将校が 2008 年 1 月初旬に、済南軍区の陸戦闘軍の小部隊が行った統合ネットワーク電子戦訓練を視察したというのがある。同電子戦訓練における防御側の PLA 兵士は、仮想攻撃軍[163]がシミュレートしたサイバー攻撃と電子攻撃をかわさなければならな

[163] 合衆国軍の演習においては、友軍(すなわち合衆国)は「青」そして敵軍は「赤」と識別される。PLA

かった。これらの攻撃には、兵站要求事項を変えるにことよって混乱をばらまくコンピュータ・ウィルスやコンピュータのマザーボード(基本部品を実装したプリント基板)を破壊する電磁パルス攻撃の利用、及び通信とレーダー・システムに対する電子妨害が含まれていた。

の演習においては、この取り決めが逆となる。すなわち、中国軍は「赤」で、敵の役割を果たす軍は「青」となる。

４　コンピュータ・ネットワーク作戦に関与する中国政府組織

４.１　人民解放軍総参謀部第３部及び第４部

人民解放軍(PLA)総参謀部の第３部は、従来からシグナル・インテリジェンス(SIGINT)収集の任務が付与されており、PLA のコンピュータ・ネットワーク・エクスプロイテーションに係る主要な責任を担っている。第３部は、これらの責任を果たすため、中国の７つの軍区の各々に「技術偵察局」を設置し、運用していると思われる。PLA 総参謀部の第４部は、従来から電子戦任務が付与されており、コンピュータ・ネットワーク攻撃における主要な役割を担っている。

本米中経済安全保障調査委員会は 2009 年、ノースロップ・グラマン社と契約し、中国のサイバー戦及びサイバー・スパイ遂行能力の新情勢について、非秘密区分指定の詳細な調査を実施させた。この「中華人民共和国のサイバー戦及びコンピュータ・ネットワーク・エクスプロイテーション能力」と題する調査報告書には、サイバー戦に関連する PLA 組織について相当詳細な内容が含まれている。この報告書は、本委員会のウェブサイトで入手可能である。

４.２　人民解放軍の「情報戦民兵」の役割

PLA のコンピュータ・ネットワーク戦に係る活動は、実戦部隊にそのすべてが限定されているわけではない。PLA は、1990 年代からサイバー民兵部隊を編成してきた。これらの部隊は、民間の情報技術セクター及び学界からの要員で構成されており、PLA コンピュータ・ネットワーク作戦と中国文民情報セキュリティ専門家との結びつきを示すものである。このような部隊が最初に編成されたのは 1998 年当初であり、山西省大同市に試験的に創設された。中国の新聞報道によれば、この大同市に創設された部隊の創設時点における要員数は 40 名であり、その場所は「大同市のある国有会社」内であるとされていた。この部隊は「地元の科学的専門知識を積んだ人物、情報技術及び設備資源」に依存しており、その要員は同市に所在する 20 の科学技術研究所、大学及び情報間連会社から引き抜かれた人物であるとされている。権威ある中国軍事科学院は 2006 年、情報戦民兵構想を明確に支持した論文を出版するとともに、PLA に対しこのような部隊を優先的に創設することを指示した。

インターネット・セキュリティ会社 iDefense による 2008 年の調査研究は、おそらくこのような民兵部隊と思われる 33 の部隊を明らかにするとともに、それらの大部分が政府の研究所、情報技術会社又は大学のコンピュータ科学部内に設置されているとした。これらの部隊に採用された人物は、年齢的に若い傾向にあり（45 歳以下)、その多くは大学教授又は院卒生若しくは民間の情報技術会社に勤務した情報技術経験を持つ者であり、さらにインテリジェンス収集に有用な外国語スキルを身に付けている者とされている。伝えられるところによれば、PLA の司令官は、価値あるスキルを持つ人物が部隊構成員として不適格とならないよう、情報戦民兵部隊要員としての標準年齢と身体的適合性要求事項を緩

めるよう指示されていた。

この他の情報源からは、政治的信頼性が要員の選定要素となっていることが指摘されている。このことに関し、権威ある軍事定期刊行物は、個々の情報戦民兵編成プロセスにおける政治的信頼性の重要性について、個々の人物の採用に当たっては「思想的認識の程度について完全に分析」することを述べている。また、選定された人物の 94%は、中国共産党又は中国共産党青年同盟のメンバーであったことが指摘されている。

中国の情報戦民兵部隊の概要

PLA は 2008 年 3 月、寧夏省永寧県に情報戦民兵部隊を創設した。この部隊の創設記念式典は地方自治体によって公表され、地方自治体の指導者は無論のこと、地元 PLA 守備隊の司令官や参謀長など当地の多数の著名人が参列した。

この時に発表された県当局ウェブ掲示によれば、情報戦民兵部隊の任務には「ネットワーク戦関連の研究と演習の強化、及びネットワーク攻撃手法の継続的改善を行うこと。・・・平時にはもっぱら敵対性ネットワークからの情報の収集を行ない、敵対性ネットワーク・データに係るデータベースを構築すること。・・・戦時には、敵対性ネットワークを攻撃するとともに、敵のネットワーク攻撃に対抗すること」が含まれている。

永寧情報戦民兵部隊の創設記念式典についての新聞報道によれば、同部隊は約 80 名の要員からなる 3 つの分遣隊から構成され、その活動の中心をネットワーク戦、情報収集と処理及びネットワーク防衛に置くとされている。同部隊の施設は「標準化された要求事項」に準拠し、オペレーション・センター、発電室、司令官室、作業室、チャート一式、その他必要な器具で構築されている。

同新聞報道は、個々の部隊要員が基本的軍事スキル及びネットワーク戦知識を含む 10 日間の基礎的な軍事訓練を受けることを明らかにしている。また、同部隊訓練に対する「3 か年進化計画」についての記述もあったが、さらなる詳細は提供されなかった。最後に、地方自治体の発表は、部隊要員の愛国心及び政治的信頼性に対する懸念についても強調したが、彼らの努力が「確固とした政治的信頼性があり、純粋な思想と社会道徳を持ち、専門職としての優秀性を備え、・・・党の宣伝を行ない、人民に利益を与え、そして情報化環境下における将来戦に勝利するための効果的な戦力を軍に提供する」部隊を構築するであろうと明言した。

４.３　「愛国的ハッカー」の役割

合衆国に向けられたサイバー攻撃の活動家として含まれる他の分類には、非公式に組織化された中国人コンピュータ・ハッカーのグループがある。彼らは「愛国的ハッカー」又は「赤いハッカー」と言われることもある。彼らは、中国の反西側感覚の国家主義とハッ

キング・スキルのテスト願望に動機付けされ、合衆国ウェブサイトに対し、際立って世間の注目を浴びる多くの「ハクティビスト」醜態化又は分散サービス妨害攻撃に係っている。これらの攻撃は、1999 年 5 月の在セルビア中華人民共和国大使館別館の誤爆、2001 年 4 月の南シナ海上における合衆国海軍 EP-3 捜索機と PLA 海軍 F-8 戦闘機の衝突後などに引き続いたこじれた米中間関係時期に、もっぱら頻繁に発生してきた。多くの中国ハッカー組織は、インターネット上で完全にオープンな活動を行い、彼ら自身のウェブページを維持するとともに、新たなメンバーをリクルートしたり、彼らのハッキング・エクスプロイト成果を自慢したりしている。中国政府は過去において、これらのグループによるハッキング活動が海外に向けられる限り黙認していた。

これらの「赤いハッカー」が中国政府からどの程度の支援や罰を受けるかについては、不明のままである。中国ハッカー・グループに関する専門家の中には、彼らは確かに非公式な組織であり、大部分は政治とは独立に活動している、と強調するような者もいる。これらの議論に関して、中国当局の観点からは「『コンピュータ・ネットワーク作戦』の一部として『ハクティビズム』を含めるとする公式の PLA 計画に対しては、いくつかの要素が反対の結論を示している」、とする論拠も強調されている。このような要素の一つは、規律の厳しい政府職員として不適である、と評価されたハッカーの性格に対する懸念である。この懸念は、情報戦民兵部隊要員選定において強く求められる政治的信頼性を強調する場合はさらに明らかとなる。その他の懸念要素には、危機の最中における赤いハッカーの予測し難い活動という特性がある。この危機の間、政府はコンピュータ・エクスプロイテーション又は攻撃の標的選定リストを管理する必要性があるだけでなく、段階的に拡大する手段と国際的世論の両者をも管理しなければならないのである。中国政府は最近、国家報道機関の社説において反ハッカーの姿勢を発表し、非公式に行われる受容できないハッカー活動を抑制する意図があることを伝えている。そして、反ハッキング法が 2009 年 2 月、全国人民代表大会において制定され、いくつかのハッカー・グループが逮捕されている。

しかしながら、これらの要素は別として、中国政府機関といくつかの個々のハッカー・グループ又はレッド・ハッカー・グループとの間に、何らかの関係があるとする明確な兆候がある。戦時のコンピュータ・ネットワーク作戦軍事行動に投入する予備役要員を、平時のコンピュータ・エクスプロイテーションやサイバー・ハラスメントに投入する必要はないはずであるが、中国はこれらタスクのある程度の実施に「愛国的ハッカー」を利用するのをいとわないように思われる。例えば、中国政府は「中国を転覆させる外国勢力に対してインターネットを介して」反撃を加える活動を奨励している。そして、赤いハッカーは、チベット支持者、新疆支持者、法輪功及び中国民主主義擁護組織のウェブサイトと所属ユーザーに対する分散サービス妨害攻撃、マリシャス・コード及びコンピュータ・エクスプロイテーション活動を正式に指図されている。さらに、少なくとも 1 人の著名な中国人ハッカーは、情報戦民兵部隊要員としてリクルートされたことが知られている。そして、国家安全部(中国の主要国内治安機関の一つ)は 2007 年～2008 年の間、中国第一流の二つ

のハッカー・フォーラム・ウェブサイト EvilOctal.com と XFocus.net の掲示板に求職情報を載せた。

これら後者の 2 つの例は、より広範な最近の傾向を物語る一部であると思われる。すなわち、最近の中国政府は、ハッカー・コミュニティから獲得することができる特殊な才能の持ち主を引き抜く努力をしつつ、また一方ではフリーランス・ハッカー活動を制限し、彼らを国家の管理下に置くことに務めているのである。この活動の一面を物語るものに、以前国家が寛大に取り扱っていた私的ハッカー・グループの情報セキュリティ会社への転換がある。この会社は、政府との密接な結びつきの下に相当な契約請負を維持している。また、中国当局は、えり抜きハッカーの逮捕という意図的に人目を引こうとした行動に及んでいる。これは、それらのハッカーが活動を継続するようであれば、彼らの活動を国家の管理下に置くという明確なメッセージを示すことを意図したものである。このような一例は、2006 年 2 月の華南省における逮捕劇に見ることができる。

> 当局は、愛国者ハッカー集団である Black Eagle Base のウェブサイトをシャットダウンするとともに、そのメンバーを逮捕した。とはいえ、そのグループは 6 か月後に活動を再開した。それと同時にそのメンバーは、グループの活動中心を国家のための要員訓練と国家のセキュリティ・ネットワークの改善に置くとする誓約を発表したのである。また、Black Eagle の指導者は、彼らが勾留されていた間に受けた教育指導に対し、国家治安局に謝意を表明したのである。

５　中国とされているサイバー・スパイの概要

その手がかりが中国にたどり着くサイバー・スパイ事件は、ビジネス、政治及び技術研究の広範な分野において注目すべき事態となっている。これらの事件には、中国少数民族と海外の反体制派グループ、合衆国連邦議会の議員室と議員及び合衆国インフラを標的としたコンピュータ・エクスプロイテーションが含まれる。それらの詳細な調査結果は、この行為が合衆国の利益に重大な潜在的脅威をもたらすだけでなく、他方面かつ常習的性格に及ぶ国家後援の中国コンピュータ・エクスプロイテーション活動の可能性を際立てさせている。

５.１　「GhostNet」

情報戦モニター(Information Warfare Monitor: IWM)の研究者達は 2009 年 3 月、広範なサイバー・スパイ・ネットワークの研究に係る極めて詳細な報告書を発表した。この IWM は、カナダのオタワに本拠地を置くシンクタンク「The SecDev Group」とトロント大学に本拠地を置く学際的な情報技術と社会科学研究所「Citizen Lab」との共同イニシアティブである。彼らによるフォレンジック調査は、彼らが「GhostNet」と呼んでいるネットワークが世界中 103 か国に及ぶ 1,295 のホスト・コンピュータに侵入したことを明らかにした。それらホストの多くは、大使館、外務省、その他の注目を引く政府機関に設置されているものであった。IWM は GhostNet 工作員の識別を決定できなかったが、GhostNet の活動パターンを取り囲む詳細な証拠は中国の関与を強く示唆するものであった。

IWM フォレンジック調査は 2008 年の夏と秋、ダライ・ラマの個人事務所、インドの Dharamsala にあるチベット亡命政府、並びにニューヨーク、ブリュッセル及びロンドンにあるチベット亡命政府が利用していたコンピュータの調査から開始された。IWM の研究チームは、E メールを介して埋め込まれた悪意のあるソフトウェア(マルウェア)により、複数のコンピュータが侵入されたことを発見した。この E メールは、専門家としての接触又は目論まれた犠牲者への政治的同情者を装ったものであった。この E メールには、添付された文書又はインターネットのリンク先のいずれかが含まれており、それらが起動されるとマルウェアがインストールされる仕組みになっていた。このマルウェアは後に、外部の管理サーバーに接続し、表題が「gh0st RAT」というリモート管理ツール(Remote Administration Tool: RAT)を含むさらなるマルウェアをダウンロードした。

「gh0st RAT」はトロイの木馬である。これにより、攻撃者はリモートからコンピュータを完全にリアルタイムでコントロールすることができる。いったん「gh0st RAT」がインストールされると、攻撃者は、他にもあるが、とりわけファイルの持ち出しやキーストローク・ログの収集を、コンピュータの正当なオペレータに認識されることなく実施することができたのである。

IWM の研究チームは、あるコンピュータに GhostNet マルウェアを意図的に感染させることにより、GhostNet ネットワークの活動を観察することができた。そして、外部サ

ーバーが、感染させられたコンピュータに命令を出しているのを明らかにした。同チームは、すべてが中国に設置された 26 の GhostNet「指揮・統制」サーバーを明らかにした。また、同チームは、GhostNet ネットワークに対するコントロール・インタフェースが中国語で行われているのを発見した。

さらに、同報告書は、中国のインテリジェンス当局がチベット亡命グループのインターネット・モニタリングと直接リンクする完全な例を、少なくとも一つ示している。それは、インドの Dharamsala にあるチベット非政府組織「Drewla」で働いていた若い女性に係る事件である。この Drewla は、2005 年に設立されたオンライン援助活動イニシアティブであり、中国語スキルのあるチベット人を雇い、若い中国人をオンライン討論に引きつけるものであった。彼女が家族を訪問するためネパールからチベットに入ろうとしたとき、彼女は逮捕され、２か月間拘留された。彼女はその間、彼女にインターネット・チャットの正確な写しを見せた中華人民共和国(PRC)インテリジェンス当局者の尋問を受けた。彼女は、彼女のグループが PRC 当局の捜査下にあり、同グループ・メンバーのチベットへの帰郷は歓迎されないと警告された。

IWM の報告書は、GhostNet に責任があるとすることについて慎重な態度を示しており、「状況証拠やその他の証拠にもかかわらず性急な判断をすること」を戒めている。とはいえ、同報告書はその結論において次のように明言している。

> 断固とした状況証拠を傾けさせる「説明」があったにせよ、この一連の注目を引かせる標的行為は、軍事的及び戦略的インテリジェンス目的で中国によって利用されたのであろう。・・・我々が明らかにした多くの信頼度の高い GhostNet による標的行為は、中国の対外政策及び防衛政策のうち、とりわけ南及び東南アジアにつながっていることが明らかである。あたかもレーダーが中国の南側国境を捜索するように、侵入された円弧は、インド、ブータン、バングラディシュ及びベトナムから、ラオス、ブルネイ、フィリピン、香港及び台湾を通過している。注目を引く標的行為のほとんどは、チベットや台湾を含め、中国を最も悩ませる対外及び安全保障政策問題に係るかなりの部分を反映したものとなっている。

GhostNet 報告の著者の一人である Rafal A. Rohozinski は、The SecDev グループの会長兼最高経営責任者であり、トロント大学の Citizen Lab の諮問委員会メンバーでもあるが、2009 年 4 月の米中経済安全保障調査委員会で証言を行うとともに、2009 年 9 月の同委員会スタッフとのフォローオン・インタビューに同意した。Rohozinski 氏は、GhostNet 活動を中国政府に属するものとして考えることに慎重な姿勢を崩さなかったが、「すべての状況証拠が、実際に、中国が運用しているネットワークを示している」と明言した。また、彼は、インターネット・プロトコル・アドレスの分析に基づき、IWM 研究チームが「高い信頼度で、攻撃者が中国の海南島に身を置いている」との確信を指摘した。

さらに、Rohozinski 氏は、GhostNet の特徴がサイバー犯罪の仕業というよりも国家後援の活動であることについても明らかにした。彼は、GhostNet ネットワークが、サイバー犯罪者が関心を持つ財務データや個人情報よりも、チベット亡命グループや行政機関などの政治的インテリジェンスの収集に向けられていたことを言及した。このような収集行為は、利益を目的とした財務詐欺行為とは異なるものである。また、彼は、GhostNet の収集手法が比較的ローテクなものであったことについても言及した。

> 「GhostNet」を介した情報収集に必要とされた要求事項は、小さな「非政府組織」より大規模なものであった。なぜかって？　　言語学的に、ラオス首相官邸、イスラエル香港領事館、ロシア北京大使館、イラン外務省を含む 103 の異なる標的行為には、何を捜し求め、それをどう考えるかを知ることができる専門知識だけでなく、言語学的スキルが要求されるからである。

分析結果によれば、情報収集に必要とされた GhostNet の手法は半熟練の個人ハッカーが入手できるようなものであったが、その収集資料の効果的な利用と分析には国家的資源が必要であることを示唆している。Rohozinsky 氏は、GhostNet のインテリジェンス収集は国家後援の活動に相当し、政府の代理としての民間の活動家によるものであることを示唆している。

我々の疑念は、これが本質的には第三者に委託された活動であって、何らかの契約上の取り決め若しくは何らかの財政的代償の保証があったかのいずれかにより、本質的に第三者が他国商船拿捕免許状と同等のものを所有し国家の合法的な海賊船となっていたのではないか、又は GhostNet のような特別な種類のネットワークを維持している見返りとしての報酬を得ていたのではないか、ということである。

この分析を支持するものとして、Rohozinski 氏は次の兆候について言及している。GhostNet は複数の攻撃者が絡んでいる。フォレンジック分析結果は、影響を受けたコンピュータが複数のマルウェアに感染していたことを示している。このことは、それが正に一つの GhostNet ではなく、複数の GhostNet であったことを意味するものである。この分析結果は、民間のハッキング・グループが政府の後援の下にインテリジェンス収集を行っていることを示すものであり、西側の有力な中国ハッカー組織分析家の見方とも一致している。また、これは、中国の代理として実施される人的スパイ及び不正な技術取得に見られるものとも一致している。そこでは、複数の民間「企業家の」活動家が活動し、たとえお互いに競合関係にあったとしても、中国の代理として情報と技術を調達するのである。（この後者の論題については、本報告書第 2 章第 3 節「合衆国を攻撃目標とした中国の人的スパイ活動とその結果が合衆国の安全保障に及ぼす影響」を参照されたい）

５.２　ほぼ確実と思われる中国の合衆国会社ネットワーク侵入の事例研究

米中経済安全保障調査委員会に提出されたノースロップ・グラマン社の報告書は、2007年に発生した匿名の合衆国ハイテク営利会社ネットワーク侵入事件に係る事例研究内容を詳しく述べている。その侵入は、中国政府とおそらくつながりがあるハッカーによって行われたものである。下記は、この事例研究の要約であり、中国のコンピュータ・ネットワーク作戦によく利用されているスパイ技術を示している。

この事例の場合、「突破チーム」と名付けられた第一のハッカー・チームが、数か月にわたり会社のネットワークを偵察した。突破チームは、作戦間におけるこのフェーズにおいて、コンピュータ・アカウント、従業員の氏名とパスワード、ネットワーク・アーキテクチャの概略などの重要な情報を入手した。彼らは、ネットワーク・ディレクトリ・マップを作成し、危殆化されたシステムに係る詳細な内容を把握した。そして、突破チームはネットワークのぜい弱性を明らかにし、それを利用した。

次に、「収集チーム」と名付けられた第二のハッカー・チームは、第一のハッカー・チームが収集した情報を利用し、会社のネットワークから機微な情報を収集した。第一チームは一般的なネットワーク攻撃ツールを利用したが、第二チームは異なるツールをまれな方法で利用している。このことは、第一チームと第二チームのオペレータが異なることを示唆している。収集を担う第二チームは、迅速かつ効率的に正確なディレクトリーに首尾よく到達し、特定の高価値ファイルをコピーした。この際、他の同じようなファイル・ネームや同じ場所にあるファイルについては、たいてい無視された。このアプローチは、第二チームが収集プロセスの間に目的としたファイルを開けることがなかったという事実に基づけば、第一の突破チームに対しては明確な任務が与えられ、その活動成果としてファイル内容の正確な識別を行ったことを示唆するものである。

第二チームは、ファイルをコピーした後、それを会社のネットワーク内にある高速の「ステージング・サーバー」[164]に転送した。これにより、会社が高価値データを記憶していると認識しているマシン上において、攻撃者の活動足跡を減少させることになる。そして攻撃者は、悪意のある活動をより効果的に隠蔽できる大容量トラフィックのマシン上に活動を集中させた。第二チームはそこで、ファイルを圧縮、暗号化するとともに、会社のネットワークから同ファイルを持ち出す前に当たりさわりのないネームを付けた。

これらの攻撃者は、見事なプロ根性とスパイ技術を展開した。彼らは、最も重要なファイルを判別し、セキュアな方法によるファイルの持ち出しを企てたのである。攻撃者はこのプロセスを通じ、攻撃活動が会社に検知されるのを避けるため、勤務時間外という特定の時間帯に活動を集中させた。攻撃者は、ファイルの持ち出しに当たり、冗長構成の通信回線を設定した。これは、同時伝送により盗み出すデータ量の最大化を図るとともに、伝

164 訳注：ステージング・サーバーとは、本番環境にアプリケーションが展開される直前に、本番と同様のテストを行うためのサーバーをいう。

送間における誤りや失敗に対する保護手段を講じたものである。また、第二チームは同時に、多くの危殆化したものではあるが正当なアカウントを利用して、会社のネットワークに 150 回以上もアクセスした。

攻撃は時々、中国に位置するインターネット・プロトコル・アドレスを持つホストから行われていた。突破フェーズと収集フェーズ攻撃の両者で利用されたツールと技法は、以前中国が関与した攻撃に利用されたものと同じであった。また、本事例において盗まれたデータの種類とその内容の特殊性からは、盗んだ情報を利用するに当たって自由裁量権のある豊富な科学技術資源を持っていると思われるエンド・ユーザーが、事前に明らかにされていることが示唆される。さらに他の要素からは、国家又は機関の関与が強く示唆される。

５.３　ほぼ確実と思われる重要インフラに対する中国のコンピュータ・ネットワーク・エクスプロイテーションと攻撃の事例

情報セキュリティ・コンサルタント業を営む The Tecnolystics 研究所の主席特別研究員 Kevin Coleman は、米中経済安全保障調査委員会に提出された証言文書において、中国のコンピュータ・エクスプロイテーション活動を警告するとともに、「石油ガス流通業者、電気通信会社及び金融企業のコンピュータ・システムにマリシャス・コードが発見されたとする報告書」を引き合いに出した。彼は、合衆国の「水処理配水システム」に対するコンピュータ攻撃の可能性について強調した。これらの問題は特に重大な懸念事項である。なぜなら、国土安全保障省が 2009 年に出版した国家インフラ防護計画は「合衆国は、政府の活動、活気ある経済及び国民の健康と安全をサイバー・インフラに依存している」と公表しているからである。これらの問題のすべては、攻撃の主要目標として表面化されている合衆国電力配電網の運用性にある程度依存している。これは、電力配電網が、他の重要インフラの能力発揮を支える役割を担っているからである。通信、金融、配水網などのすべてのインフラが、電力を必要としているのである。

悪意のある活動家は、より着実なエクスプロイテーション情報を取得するため、これらの徹底的な調査を利用する。Wall Street Journal は 2009 年 4 月、合衆国電力配電網やその他の重要インフラ・ノードに対する侵入の蔓延について報告した。同報告によれば、これらのネットワーク突破の中には、侵入者がリモートから起動させた場合に対象システムを混乱又は破壊することができるソフトウェアを埋め込んだものがあったとしている。Wall Street Journal は、この捜査に関与したインテリジェンス当局者を引き合いに出して、同侵入の主役が中国であることを明らかにした。合衆国は既に、中国によるインフラ制御装置のエクスプロイテーション結果を、甘んじて引き受けているのかもしれない。National Journal は 2008 年 5 月、2003 年と 2007 年にそれぞれニューヨークとフロリダで発生した停電の原因が、中国のサイバー攻撃によるものであったかもしれないと公表した。

重要インフラに対する攻撃は、危機又は戦争時に優勢を獲得するために利用することができる。とりわけ、このような攻撃目標を探し求めることは、権威あるコンピュータ・ネットワーク作戦に係る人民解放軍(PLA)の文書に一致している。中国のサイバー戦慣行の専門家である James Mulvenon によれば、中国の分析家は「非軍事目標に対するコンピュータ・ネットワーク攻撃は『戦争の決意をぐらつかせ、戦闘能力を破壊し、戦争における優勢を勝ち取るための』ものであり、これにより軍事紛争への参加に対する全住民の政治的意思を徐々に衰えさせる」と明言している、と述べている。

５.４　ほぼ確実と思われる合衆国議会に対する中国のコンピュータ・ネットワーク・エクスプロイテーションの事例

2008 年 12 月、合衆国下院において 2006 年のコンピュータ侵入報告が明るみにされた。調査者は、8 人の連邦議会議員と 7 つの米国連邦議会委員会の情報システムが危殆化されたことを確認した。これらの攻撃に利用されたマルウェアは、回りくどいルートをたどった後、中国にあるサーバーとの接続を確立しようとしていた。同攻撃の報告は中国政府と直接リンクする寸前で中止されたが、詳細な情報は政府との結びつきがありとせざるを得ないと示唆するものであった。例えば、フォレンジック・データは別として、標的目標にされた連邦議会議員は、計り知れない政治的価値のある情報を持っていたものの、本質的に犯罪価値がある情報については持っていたとしてもほんのわずかだったのである。攻撃された議員には、下院議員の Frank Wolf（共和党、バージニア州）と下院議員 Mark Kirk（共和党、イリノイ州）がいる。Frank Wolf は、人権擁護グループと民主主義擁護活動と長年に及ぶつながりのある下院議員である。Mark Kirk は、当時米中作業グループの共同議長を務めていたが、とりわけ、二国間貿易問題に取り組んでいた。

少なくとも上院議員の一人は、彼の事務所のコンピュータ・システムがサイバー侵入されたことについて抗議すると発表した。上院議員の Bill Nelson は 2009 年 3 月 19 日、上院軍事委員会の聴聞会において、「先月、私のオフィスのコンピュータが 3 回も侵入された。我々は、その一つが極めて重大と考える」と明言した。上院議員 Nelson の補佐官は、インターネット・プロトコル・データの分析によれば、攻撃の発生源が中国であったと指摘した。

６　結論

✧　合衆国に対する悪意のあるコンピュータ活動の量は、2008 年に増加し、2009 年には急激な増加となっている。この活動の大部分は、中国から発生したものと考えられる。

✧　合衆国を攻撃目標としたこのような活動に対する中国の直接関与を明らかにすることは、ハッカーによる彼らの所在隠蔽能力の高さから難問を呈している。それでもなお、ますます増え続けるかなりの量の状況証拠やフォレンジック証拠は、中国の関与と国家後援組織による攻撃であることを強く示している。

✧　中国政府は、人民解放軍部隊内にコンピュータ・ネットワーク作戦に係る多くの能力を組織化している。また、中華人民共和国は、同国のサイバー能力を高めるため、ますます人口が増加している同国の技術的にスキルの高い人々をリクルートしている。このリクルート対象には、民間セクターの技術者も含まれる。中国は、情報技術会社やコンピュータ科学プログラムからスキルの高いオペレータをリクルートし、多数の情報戦民兵部隊に投入しつつある。

✧　中国の平時におけるコンピュータ・エクスプロイテーション活動は、合衆国の標的と海外の中国反体制グループに対するインテリジェンス収集活動に、その焦点が当てられている。

✧　人民解放軍は紛争の初期段階において、敵対する政府と軍情報システムに対してコンピュータ・ネットワーク作戦を利用するであろう。

✧　合衆国の重要インフラは、悪意のあるサイバー活動にぜい弱である。中国軍のドクトリンは、紛争時にこれらのぜい弱性を利用することを求めている。

平成２１年・２２年発刊・発刊予定資料

ＢＳＫ 第２１－　１号『我が国をめぐる兵器技術情報管理の諸問題（平成２０年度）』

ＢＳＫ 第２１－　２号『米国における情報システムの不測事態対応計画について(平成 20 年度)』

ＢＳＫ 第２１－　３号『外国の経済情報収集および産業スパイ活動に関する議会への年次報告(2007 年度)』

ＢＳＫ 第２１－　４号『新しい防衛調達モデルの探索的調査研究（その２）』

ＢＳＫ 第２１－　５号『中央政府における究極の省庁別財務責任者である会計官、主席財務官等の役割に関する国際比較研究』

ＢＳＫ 第２１－　６号『多層防衛：セキュアで弾力性のあるＩＴ組織の礎』(保全講習受講用)

ＢＳＫ 第２１－　７号『インサイダー脅威の防止・探知のための共通ガイド第３版』『米国の国家対情報戦略(2008 年)』

ＢＳＫ 第２２－　１号『標　的　に　さ　れ　る　合　衆　国　技　術』

ＢＳＫ 第２２－　２号『我が国をめぐる兵器技術情報管理の諸問題（平成 21 年度）』

ＢＳＫ 第２２－　３号『カウンターインテリジェンスの最前線に位置する防衛関連企業の対策について(平成 21 年度)』

ＢＳＫ 第２２－　４号『新しい防衛調達モデルの探索的調査研究（その３）』

ＢＳＫ 第２２－　５号『中華人民共和国のサイバー戦とコンピュータ・ネットワーク・エクスプロイテーション能力』
『米中経済安全保障調査委員会議会報告 2009 から抜粋』

中華人民共和国のサイバー戦とコンピュータ・ネットワーク・エクスプロイテーション能力

（米中経済安全保障調査委員会への提出資料）

米中経済安全保障調査委員会議会報告　２００９から抜粋

第２章 合衆国の安全保障利益に直接影響を及ぼす中国の活動

第３節 合衆国を攻撃目標とした中国の人的スパイ活動と合衆国国家安全保障に及ぼす影響

第４節 合衆国を攻撃目標とした中国のサイバー活動と合衆国国家安全保障に及ぼす影響

平成２２年９月　発行
非 売 品　　禁 無 断 転 載・複 製
発　　行　：　財団法人　防衛調達基盤整備協会
編　　集　：　防衛調達研究センター刊行物等編集委員会
〒160-0003　東京都新宿区本塩町２１番３－２
電　話　：　０３－３３５８－８７５４
ＦＡＸ　：　０３－３３５８－８７３５
メール　：　hozen@bsk-z.or.jp
ＢＳＫホームページ：　http://www.bsk-z.or.jp