連　載
第７回

情報と防災

防衛大学校安全保障・危機管理教育センター長
教　授　太　田　文　雄

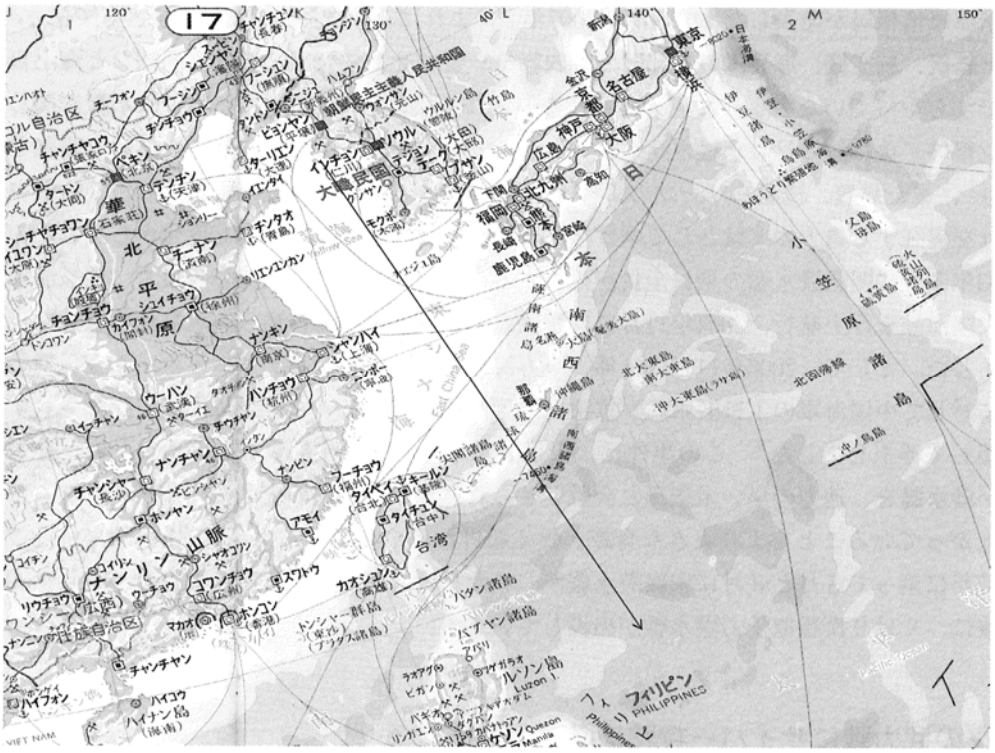
2008 年暮れに生起したインドの同時テロに関しては、インドの情報機関 RAW がパキスタンのカラチにあるラシュカレトイバの拠点から発信された「貨物船が目的地に向かっている」との衛星電話での会話を傍受、治安部隊や海軍などに連絡したり、ムンバイの漁業組合が四カ月前に爆薬を積んだ漁船がムンバイに入港したといった情報を当局に知らせたのにもかかわらず無視されたといった報道が出ていました [1]。そこで、今回は「過去の兆候からインテリジェンスを組み立て、現在発生、あるいは将来起こりうる事象を予察する」という作業を最近発生した問題を例に挙げて説明していきたいと思います。

北朝鮮とイラン

平成 20 年 9 月 12 日(金)の新聞に、北朝鮮が黄海沿岸に、新たなミサイル発射施設を建設中として衛星写真付きの記事が出ました。これまで、北朝鮮の弾道ミサイル発射試験は 1993 年 5 月のノドン、1998 年 8 月のテポドン 1 号、2006 年 7 月のテポドン 2 号を始めとする連続 7 発の発射と、全て東岸から日本海に向けて発射されたものでした。何故、北朝鮮は、今回西岸の黄海沿岸に弾道ミサイル発射施設を建設したのでしょうか?

それは射程 1,000km を越える弾道ミサイルを東岸から発射すると必ず日本の上空を飛び越え、1998 年 8 月の時のように「日本政府が情報収集衛星を打ち上げる」といったリアクションを引き起こし、それを嫌う中国との関係もまずくなるからだと思います。従って、次頁の図のように韓国と日本の南西諸島の上空に掛からない極めて細い回廊に向けて試験発射を試みようとしているのではないでしょうか?

また 11 月 13 日(木)の新聞に「12 日、イランが射程 2,000 ㎞以上の弾道ミサイルを発射した」という記事がでました。欧米の新聞では「このミサイルは固体燃料を使用している模様である」と報じています [2]。これが事実であるとすると、これは将来かなり大きな問題となります。と言いますのは、イランが固体燃料の弾道ミサイルを保有したとなると、その技術は北朝鮮にも渡る可能性が極めて高いからです。



現在北朝鮮が日本を射程におさめる弾道ミサイルは全て液体燃料であり、固体燃料の弾道ミサイルは保有していません。液体燃料の弾道ミサイルであれば燃料注入に時間がかかり、発射準備をしている間に偵察衛星などで発見できる可能性が高いのですが、固体燃料の弾道ミサイルとなると、発射までの時間が極めて短いため警告時間が短くなり、ミサイル防衛が難しくなります。

イランと北朝鮮の弾道ミサイルに関するやり取りに関しては、過去に複数の報道がなされています。例えば 2006 年 4 月に前米国務省東アジア太平洋顧問のデーヴィッド・アッシュアー氏が、北朝鮮がイランに射程数千キロの旧ソ連の SS-N-6 を改良した BM25 を 18 基輸出したと証言していますし[3]、その翌日にはイスラエル軍の情報部長が、その事実を認めています[4]。2008 年 4 月 17 日の新聞にはイランの長射程弾道ミサイル発射施設の衛星写真が出、これが北朝鮮の長距離弾道ミサイル発射施設と酷似していると報道されています[5]。

土佐沖の潜水艦らしきもの

10 月 14 日に土佐沖の領海で潜水艦らしきものが発見されました。その後の調査では「潜水艦かどうかも不明」ということでしたが、仮に、これが潜水艦であったとしたら、私は過去の兆候から中国の潜水艦である可能性が高いと思っています。

米海軍情報局が発表した「中国海軍 2007 年」によれば、訓練面で 2002 年を境として潜水艦、水上艦艇、航空機、海兵隊の各部門とも内容を一変させ、荒天下における訓練など海上自衛隊ですらやっていないような極めて高度なレベルを実施しています 6。特に潜水艦に関しては攻撃終了後に敵の対潜水艦ネットワークから安全に突破することに焦点を置いた訓練をしたり [7]、また島嶼、浅瀬、リーフのような狭隘、浅海における通過訓練を開始しています [8]。

これを実証する過去の兆候として挙げられるのが、訓練レベル要求の高度化から生じたのか 2003 年 5 月に明級潜水艦の乗員全員が死亡する事故が起き、その後 2003 年 11 月に明級潜水艦が大隅海峡を浮上航行、2004 年 11 月には漢級原子力潜水艦が宮古島・石垣島間の領海を侵犯しました。そして、2006 年 11 月には沖縄東方海域を航行中の米キティー・ホーク空母機動部隊に対して中国海軍の宋級潜水艦が魚雷発射可能距離である 5 マイル以内まで探知されずに近接して浮上しました [9]。この事件は、宋級潜水艦の能力に注目するというよりも、速力の遅い潜水艦を、速力の早い米空母と会敵させられるような中国の広域海洋監視システムが出来上がっていることをより大きな脅威と捉えなければなりません [10]。この先島諸島付近では 2007 年に至って 5 月と 8 月に宋級潜水艦が、また日米共同演習が行われた 11 月 9 月及び 20 日前後に、やはり漢級原子力潜水艦が出没しています。

将来の武力戦にサイバー攻撃は必ず併用される

2008 年 8 月に生起したロシアとグルジアの軍事衝突の約 1 カ月前からグルジアはロシアのサイバー攻撃を受けたとされています [11]。また、2008 年 11 月 28 日のロスアンゼルス・タイムズには「ロシア国内から米国防総省にサイバー攻撃がかけられている」という記事が出ていました [12]。

サイバー攻撃とは、コンピューター・ネットワークを通じて各国の国防・治安等にかかわるコンピューター・システムに対し、侵入、データの破壊、改ざんなどを行い、国家又は社会の重要な基盤を機能不全に陥れる行為です。重要な基盤とは公共施設である電気通信ネットワーク・システム、電力システム(発電所、送配電・燃料輸送・貯蔵施設)、ガス・石油の生産、貯蔵、輸送施設、金融、運輸、給油システム、緊急サービス(救急医療、警察、消防等)、そして行政機能などが挙げられます。特に日本のような経済大国の場合、日銀のシステムが麻痺することは全世界に対する信用問題にも発展します。

サイバー攻撃の特性としては第一に地理的・時間的制約がないこと、第二に匿名性・無痕跡性を有しており否定しやすいこと、そして第三に攻撃に要するコストやリスクが低いことが挙げられます。

戦争を決定づけるファクターが情報力となり、ネットワーク・セントリックに戦いとなってきますと、敵を攻撃するには、そのネットワークを攻撃することが極めて有効な手段となってきます。私が知る範囲で、これを最初に実行したのは米国で、湾岸戦争の時イラクの防空システムに

対して行っています。また 1996 年にはボスニアで、1999 年にはコソボでセルビア軍の防空システムに対してサイバー攻撃をかけました。2000 年 1 月に日本政府の官公庁ホーム・ページが改竄されたことは有名ですが、翌 2001 年 4 月 1 日に米海軍の EP-3 が海南島に強制着陸させられた直後、中国のサイバー攻撃が米国に対してなされました。最近では 2007 年にロシア戦士の碑を撤去しようとしたエストニァに対してロシアが、さらにイスラエルがシリアの核疑惑施設を攻撃した際も、サイバー攻撃を併用したと言われています。日本でもいわゆるサービス停止(DOS)攻撃を 2004 年 8 月、2005 年 4 月、2006 年 8 月に受けました。従って、将来戦においては、武力攻撃に並行してサイバー攻撃も行われることが状態となってくることを認識しておかなければならないと思います。中国が尖閣列島や台湾に侵攻する際、サイバー攻撃を併用する可能性は高いものと思われます。

サイバー攻撃は我が国では法律で禁止されており、もちろん要員養成などもできない状態ですが、我が国周辺国の中にはコンピューター・ハッカーの専門部隊を育成して、対象国政府組織内のコンピューターに進入、メモリーの中身を盗み出すという努力を行っている国があると言われています。例えば、米国防省発表、『2008 年中国の軍事力』には 2007 年に中国人民解放軍を発信地とする多重のコンピューター・ネットワーク侵入が米国防総省、他の米政府省庁、防衛関係シンク・タンクや契約会社にかけられ、さらにこうした攻撃はドイツの国内インテリジェンス機関の副所長 HansElmarRemberg 氏にほぼ毎日、フランス国防官房長の FrancisDelon 氏に、また英国の企業にもかけられたことからインテリジェンス組織 MI5 の JonathanEvans 長官は 300 の財政組織幹部に警告を発しています[13]。

2008 年 11 月の米大統領選挙の直後である 11 月 7 日の『フィナンシャル・タイムズ』には「中国がホワイト・ハウスのネットワークをハッキングした」との見出しで記事が出ました[14]。

中国は1997年に網軍と呼称する約40万の人員で24時間ネット監視を開始し始めるとともに、同年約 100 人規模のコンピューター・ウイルス部隊を創設しました。1999 年にはハッカー部隊を創設、2003 年には北京に情報化部隊を創設しました。2004 年から 2005 年の間に北京以外の 6 軍管区でも攻防両面の情報戦を遂行する目的を持った特別技術偵察隊(STRU)を創設しました。2007 年の評価では、中国は敵意のある暗号適用、電子回路破壊能力、自動暗号化・敵意暗号の解読、ワイヤレス・ネットワークの外部からの破壊能力、共通商用ソフト内の未報告脆弱性の利用といったことを「高度データ兵器」として使用する能力を開発している模様です[15]。

このようにして 1999 年に喬良、王湘穂という二人の中国空軍大佐が共著で出した、いわゆる「超限戦」(武力も非武力も、軍事的も非軍事的も、殺人や傷害またそうでないものも含め、あらゆる手段を用いて自分たちの利益を敵に無理やり認めさせる)を推進しているといわれています。現に 2000 年の 1 月から 2 月にかけて日本の 19 省庁のホーム・ページが不正アクセスを受けた、というニュースは記憶に新しいところです。情報に依存しすぎている西側に対し衛星破壊はハード・キル、サイバー攻撃はソフト・キルという位置づけなのでしょう。

また 2004 年 10 月 4 日の『中央日報』には「北朝鮮ハッカー500～600 人余が活動中」という見

出しで「米国や日本など敵性国家の軍事情報の収集、軍の指揮や通信網の撹乱などハッキングとサーバー戦争を遂行する任務を受け持っている」といった記述が見られます。

北朝鮮は1990年以降金一大学及び美林自動化大学に毎年約100人のサイバー担当者を養成し、2000年には麻痺計画を作成、約600人でハッカー部隊を編成した模様です。そして2001年頃、全国からコンピューターに関する秀才約 600 人を集め、2002 年にはサイバー心理部隊を新編しています。2006年7月に北朝鮮が弾道ミサイルを発射した際、同時に北朝鮮の121部隊と呼ばれるサイバー部隊が韓国と米国防総省に侵入してサイバー攻撃を掛けた、と米国防総省当局者がAP通信とのインタヴューで概要を語っています。

防衛省は各自衛隊にコンピューター・システムの防護(監査)隊を設け、また 2007 年度末には統幕に自衛隊指揮通信システム隊を新設して情報保証に努めていますが、私は今から約 10 年前の1998年に米国の武官団旅行でテキサス州のLackland空軍基地にある航空インテリジェンス局(TheAirIntelligenceAgency)と統合指揮通信(JointCommandandControl)施設を研修し、当時から米軍が莫大な人員と資源を投じてサイバー攻撃対処に努力しているかを目の当たりにしてきました。その米国ですら 2005 年夏に中国企業レノボ(IBM パソコン部門を買収)からのパソコン購入を全面的に取り止め、2007年9月にマイケル・ウィン空軍長官がサイバー戦司令部新設宣言を出したほどです。米国は、2007年8月末から9月初めにかけて受けた中国からのサイバー攻撃に対し、当初2.5万人いた対策本部を9月に3.8万人、12月には4.6万人として中国の7万人(研究開発体制をも含めると約十万人)とも言われる体制に対抗すべく急速に増員されています。

2008年8月に在日米軍司令官と話した際、彼も「将来の武力戦にサイバー攻撃は併用される」という私の意見に同意してくれ「米軍では現在空軍少将がトップで担当しているサイバー空間での戦いを中将が指揮する統合の組織に昇格しようとしている」として、米軍の熱心な取り組みを説いてくれました。

1 産経新聞「インド同時テロ政府批判強まる複数の事前情報無視」、平成20年12月2日

2 BritHume,IranTest-FiresMissile,FCN,November12,2008

3 産経新聞、2006年4月27日

4 産経新聞、2006年4月28日

5 産経新聞、2008年4月17日

6 China'sNavy2007,pp.37(潜水艦)、43-44(水上艦艇)、49-50(航空機)、56(海兵隊)。

7 China'sNavy2007,p.37.

8 China'sNavy2007,p.90.

9 Bill Gertz,ChinaSubSecret/yStalkedU.S.Fleet,TheWashingtonTimes,November13,2006

10 NormanFriedman,BackintheSurvei/lanceGame,USNavalProceedings,January2007,pp.9091.

11 JohnMarkoff,"BeforeTheGunfire,Cyberattacks",NewYorkTimes,August13,2008,p.1

12 John Markoff,Before The Gunfire,Cyberattacks,New York Times,August13,2008,p.1

vember28, 2008, Pg. l

13 OfficeoftheSecretaryofDefense, Mi!itaryPowerofthePeople'sRepub/icofChina2008, p. 3^, 4.

14 DemetriSevastopulo, ChineseHackIntoWhiteHouseノTet2vork, FinancialTimes, November7, 2008.

15 KevinColeman, CyberThreatMatrix, DefenseTech. orgwebpage, December2007,

http://wwwdefensetech. org/archives/2007_12. htm1