Vol.2013-EIP-62 No.8
2013/11/21

人民解放軍のサイバー戦における民間能力活用に関する一考察

倉持一[†1]　平塚三好[†2]

2009 年 10 月に公表された米中経済安全保障調査委員会の年次報告は，中国のインテリジェンス活動の増大，その中でも特に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や，それらの活動に国家的関与が窺われることなどを指摘している．また，2013 年 2 月，米国コンピュータ・セキュリティ企業は，主に米企業を標的とするハッカー攻撃を中国政府が支援している可能性が高い集団が行っていることや，攻撃母体の一つが上海市内に所在する人民解放軍の秘密サイバー部隊であることなどを指摘する報告書を発表した．

両報告書では見落とされているが，中国のサイバー戦を論ずる際には「民間能力活用」という観点は欠かせない．それというのも，中国は，江沢民の情報化戦略を具体化すべく，サイバー戦に向け民間能力を「民兵」や「協力者」として組織化しているからだ．例えば人民解放軍は，高度な IT 技術を有する民間人らを集め，また，民間の「愛国ハッカー」を重要な国家資源として位置づけ，当局の統制下・指揮下におくことでその能力を活用している．以上のとおり，中国は，サイバー戦に向けた民間能力活用のため，国家総動員的な資源集約を図っているが，特に人民解放軍の動向には今後も注目を要する．

A Study on the use of civilian capabilities in cyberwar of the People's Liberation Army

HAJIME KURAMOCHI[†1]　MITSUYOSHI HIRATSUKA[†2]

The annual report of U.S.-CHINA ECONOMIC and SECURITY REVIEW COMMISSION announced in October 2009 has pointed out that Chinese activity using a cyberspace is activating and the thing about which national participation asks those activities. Moreover, the U.S. computer security company released the report in February 2013 which pointed out that a possibility that the Chinese government is supporting the hacker attack to a U.S. company is high and that a secret cyber-unit of the People's Liberation Army in Shanghai carried out it.

Although it misses in both reports, when discussing a cyberwar of China, the viewpoint of "civilian-capabilities practical use" is indispensable. It is because civilian capabilities are systematized as a "militia" and a "cooperator". China is going to materialize Jiang Zemin's information strategy.

For example, People's Liberation Army gathers the civilians who have advanced IT technology and positions private "patriotic hacker" as important national resources. As above, We have to note that China is carrying out civilian-capabilities practical use towards cyberwar.

1. はじめに

2009 年 10 月に公表された米中経済安全保障調査委員会の年次報告は，中国のインテリジェンス活動の増大，その中でも特に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や，それらの活動に国家的関与が窺われることなどを指摘している．また，2013 年 2 月，米国コンピュータ・セキュリティ企業は，主に米企業を標的とするハッカー攻撃を中国政府が支援している可能性が高い集団が行っていることや，攻撃母体の一つが上海市内に所在する人民解放軍の秘密サイバー部隊であることなどを指摘する報告書を発表した．

両報告書における仔細な指摘にもあるとおり，中国は国家的な指揮・指導の下で，サイバー戦に対応する組織体制の整備を図っているが，両報告書で抜け落ちているのが，人民解放軍による「民間能力活用」という視点である．後に詳しく考察するが，人民解放軍は時の最高指導者の掲げる軍事戦略に従い，その能力や組織を拡大ないし精鋭化してきたが，特に近年では，サイバー戦に備えた動きを活発化させていることが認められる．

この背景には，戦争の空間が，陸と海に始まり，空から宇宙，さらにはサーバー空間へと技術の進歩とともにその領域を広げており，いまやサイバー空間は「第 5 の戦場（①陸，②海，③空，④宇宙，⑤サーバー空間）」と呼ばれるようになってきている[1]という事情があろう．そして，このサイバー戦においては，集合的な肉体的鍛錬や高度な技術訓練を必要とする歩兵や戦闘機パイロットのような従来からの戦場に対応した兵力，すなわち正規の軍人の能力だけでなく，民兵の組織化や民間企業の協力獲得といった，所謂「民間能力の活用」がキーポイントになってくると考えられる．

筆者が確認した限り，既に 2000 年には，米中央情報局（CIA）のセラビアン情報作戦担当官と国防大学のクエール教授が，上下両院合同経済委員会の公聴会において，中国が来るべきサイバー戦に備え「電脳攻撃戦略」を開発し

†1 立教大学大学院
Rikkyo University
†2 東京理科大学
Tokyo University of Science

ていると指摘している[2]．さらにそれ以降も，2006 年 2 月[3], 2007 年 9 月[4], 2008 年 3 月[5], 2009 年 4 月[6], 2010 年 1 月[7]および 2 月[8]，2011 年 10 月[9]および 11 月[10]，2012 年 9 月[11]および 11 月[12]，2013 年 2 月[13]および 3 月[14]などにも，米国の政府高官らが人民解放軍によるサイバー攻撃の脅威について注意喚起を促すような発言を行っている．中でも，米国コンピュータ・セキュリティ企業のディアマント社は，上海に拠点を置く人民解放軍「61398 部隊」が，2006 年頃から中国によるサイバー攻撃の主導的役割を果たしているとして，部隊の所在ビルを特定した上で指摘した[15].

この様に，情報技術の発展により，中国のサイバー戦に人民解放軍が深く関与していることがより明確となってきている．しかし，人民解放軍のサイバー戦の矛先は米国だけに向いているのではない．杉山徹宗は,「戦略戦力を外国に依存している日本としては，隣の中華帝国の軍事増強政策に対して，常に詳細な情報を入手し，その動向を注視しつづけるとともに，日本の平和と繁栄が乱されないよう，万全の備えを立てておく必要が有る」[16]と述べているが，本研究は，まだ本格的な研究対象とはなっていないアジアの大国，かつ，我が国の隣国である中国の人民解放軍のサイバー戦に向けた組織整備実態，その中でも特に，民間能力活用による国家総動員的側面などに焦点を当てて考察し，主に我が国の今後の危機管理の一助となることを目的としている．

2. 人民解放軍の戦略変化

国家の軍隊ではなく中国共産党の軍隊である人民解放軍であるが，その指揮権は軍権の最高意思決定機関である中央軍事委員会にある．そして，同委員会を統帥するのが中央軍事委員会主席なのであるが[17]，中央軍事委員会は主席責任性を採用しており，多数決ではなく主席が最終決定権を有している[18].

ではここで，現代のサイバー戦に向けた人民解放軍の体制整備に至る経緯や背景事情などを理解するためにも，時の最高権力者である歴代の主席がこれまでに打ち出した人民解放軍の戦略を確認し,その歴史的展開を明らかにする．

(1) 鄧小平時代

鄧小平は，1973 年，文化大革命で失脚していたものの復活し,1975 年 1 月 5 日には人民解放軍総参謀長に就任した．彼は，同月 25 日に開催された総参謀部・機関・連隊以上の幹部会議で「軍地を改革しなければならない」ことを指示し，ついで同年 7 月の中央軍事委員会拡大会議において，軍隊の改革に関する自らの考え方を説明した．それらの発言において鄧小平は，兵員の大幅な削減による人民解放軍の近代的軍隊への全面的な改革を提起した[19].

鄧小平の軍事改革は，1978 年に本格的にスタートするが，まずは，同年 12 月の中国共産党第 11 期 3 中全会において文化大革命の指導理念であった毛沢東の「継続革命論」を否定することで人民解放軍の戦略を毛沢東のそれから解放し，党の活動の重点を経済建設へと移すことで，軍の近代化・正規化の先鞭をつけた．この鄧小平の軍事改革の前提には，人民解放軍が主なプレーヤーとなる戦争は，当分の間は生起しないという認識が存在していた[20].

なお，鄧小平は，1981 年に中央軍事委員会主席に就任するが，以後，1989 年に同職を辞するまで，党総書記や国家主席に就任することはなく最高権力者として軍の近代化を押し進め続けた．

(2) 江沢民時代

鄧小平による人民解放軍のスリム化と近代化という流れは，次の中央軍事委員会主席である江沢民にも引き継がれた．1997 年，江沢民・中央軍事委員会主席は，今後 3 年間で人民解放軍の兵力を 50 万人削減する方針を打ち出した[21]. 1985 年の統計によれば，人民解放軍の総兵員数は 450 万人であったが，その後の 2 年間で 100 万人が削減され，結果として約 350 万人にまで減少していた．江沢民は，これをさらに 50 万人削減して総兵員数を 300 万人にしようとするものである[22].

鄧小平に倣い人民解放軍のスリム化に着手した江沢民であったが，その主眼はやはり近代化にあった．特に，人民解放軍は，1991 年に発生した湾岸戦争における近代戦闘を目の当たりにし，さらなるハイテク化の必要性を痛感したものと考えられる．実際，1993 年 5 月 20 日，江沢民の腹心である劉華清・中央軍事委員会副主席は，中国共産党幹部を養成する中央党校において「中国的特色をもつ現代化軍隊の建設」についての報告を行っている．

同報告においては，①国際戦略情勢と中国周辺の環境から勘案すると，全面戦争の可能性は大きくないが，軍隊の現代化水準は依然高くないので 300 万人規模の軍隊の保持は必要である，②我が国は海に面する大国であり，数百万平方キロメートルにおよぶ海域を持っている．海洋権益を守るためにも強大な海軍を建設すべきである，③現代戦争は，海上作戦であれ航空作戦であれ，空軍の支援が必要である．それゆえ，海軍，空軍の現代化を優先しなくてはならない,④湾岸戦争はハイテク戦争の特徴を体現している．しかし，いかなるハイテク・システムにも弱点はあるのだから，それに対処する方法を探らなければならない．未来のハイテク戦争においても，劣勢な装備で優勢な装備の敵に打ち勝つという人民解放軍の伝統を発揮しなくてはならない，といった点が指摘されている[23].

つまり，鄧小平の軍事改革によってスリム化と近代化の道を歩んできた人民解放軍は，1991 年の湾岸戦争における米軍を中心とした近代のハイテク戦争の圧倒的戦力の誇示を契機として，人民解放軍のハイテク化という新たな方針へと戦略の舵を修正したのである．

(3) 胡錦濤時代

胡錦濤は 2002 年の第 16 回党大会で江沢民の後任者として党総書記に就任したが，中央軍事委員会主席のポストは江沢民が手放さず，胡錦濤が就任したのは党総書記の就任から約 2 年が経過した 2004 年 9 月になってからであった．ただし，胡錦濤は，中央軍事委員会主席に就任する直前の同年 7 月に，党中央政治局集団学習会で「経済建設・国防建設」を取り上げ，国防建設と経済建設とを同時並行させる考え方を明確にした[24]．また，胡錦濤は中央軍事委主席就任と同時に組織改編を行い，海軍，空軍，第二砲兵の各トップである司令員を中央軍事委員会のメンバーに新たに加えた．これには，伝統的に陸軍が圧倒的に優位だった人民解放軍の組織を，世界で主流になりつつある陸・海・空軍の三軍統合運用と戦略核兵器の維持という最新の軍事戦略に適合できる組織へと変化させるという意図があったと考えられる．

ただし，胡錦濤の軍事戦略は，鄧小平による大胆な兵員削減と軍の近代化，江沢民による軍のハイテク化，そして情報化への先鞭といった，戦争の形態を変容させるような大きな変化は生じていないとされる[25]．とは言え，胡錦濤政権下の 2011 年には，中国は GDP 規模で世界第 2 位の経済大国へと伸長しており，それによって確保した豊富な軍事予算を用いて，軍の情報化を確実に進展させていった．

胡錦濤の押し進めた軍事戦略の特徴の一つには，「軍人のプロフェッショナル化」がある．日進月歩の勢いで発展する最新の情報技術を人民解放軍に取り入れるためにも，軍人のプロフェッショナル化は避けては通れなかったと思われる．胡錦濤による中国共産党第 17 回党大会報告では，「情報条件下の軍事訓練」，「人材育成システム」，「民兵の資質強化など，後備兵力の人的素養の強化」などが呼びかけられた[26]．

すなわち，胡錦濤は江沢民が推進した軍や兵器のハイテク化をさらに一歩進めて情報化へと発展させるのと同時に，今後想定される戦争の空間の概念拡大に対応するための後備兵力を含めた人民解放軍全体のレベルアップを志向したと言えるだろう．

(4) 習近平時代

大方の事前予想に反し，2012 年 11 月に胡錦濤は，党総書記のポストのみならず党中央軍事委員会主席のポストも同時に習近平へ禅譲した．よって，おそらくは，2012 年から 2022 年までの 2 期 10 年間は，習近平が中国共産党と人民解放軍のトップとして君臨することが予想される．

習近平は，早速，中央軍事委員会をはじめとする軍幹部の人事に着手したが，現場の部隊運用のトップとなる総参謀長には，それまで北京軍区司令員を務めた房峰輝・上将を指名した．彼は，首都・北京の防衛を受け持つ北京軍区での活躍により胡錦濤の信頼が厚かったとされ，また，近代戦に必要なハイテク装備やサイバー戦にも造詣が深いとされている[27]．

また，退任する胡錦濤が今後 5 年間の党運営の方向性を打ち出した 2012 年 11 月の中国共産党第 18 回党大会報告では，国防部分において「三段階戦略構想」が謳われている．中央軍事委員会主席が習近平に交代しても，この党大会報告は引き続き，党の軍隊である人民解放軍の戦略を基礎づけることに留意が必要である．

同構想自体は 2009 年に発表されているが，①2010 年までに軍建設の確固たる基礎を築き，②2020 年までには概ね機械化を実現し，また情報化においても大きな発展を成し遂げ，③2050 年ころまでに軍の近代化の目標を基本的に完成する，という軍事戦略構想である[28]．さらに同報告では，軍事戦略に関して，「サイバー空間」，「機械化と情報化」，「情報化条件下の局地戦に勝利する能力」，「確固不動たる情報化を軍の現代化建設の発展方向とし，情報化建設の発展を押し進める」など，情報化こそが人民解放軍の目指す道であることや，サイバー戦に備える必要性などが強調されている[29]．

総参謀長人事や党大会報告にも表れているように，胡錦濤の後を継いで中央軍事委員会主席に就任した習近平時代の軍事戦略の特徴は，人民解放軍の情報化の進展と実行力向上，すなわち，近年現実化したサイバー空間での攻撃および防御能力の向上にあると言えるだろう．しかし，昨今の人民解放軍のサイバー戦（主に攻撃面）については，米国がそれまでの静観姿勢から，2013 年 6 月の米中首脳会談において「両国関係の発展の妨げになる」と懸念を表明するなど[30]，新たな外交的ないし軍事的な脅威と捉えられている．

3. サイバー戦に向けた人民解放軍の組織体制

人民解放軍の戦略変化を歴史的に俯瞰し，その近代化と情報化への流れを理解したところで，本章では，現在の人民解放軍がいかにしてサイバー戦に備えた組織整備を図っているのかについて確認していきたい．

ちなみに中国では，軍事力を「武装力量」と総称している．主力は正規軍の人民解放軍であるが，準軍隊として存在する中国人民武装警察部隊と大衆武装組織の民兵も武装力量としている．これらを合わせて，「三結合」の武装力と呼ばれている．

	常備兵力		後備兵力
三結合	人民解放軍	武装警察	民兵

図 1　中国の軍事力の概念

そして，人民解放軍総参謀部電子対抗雷達部の部長を努めた戴清民は，サーバー戦を，①「作戦保密」，②「軍事欺瞞」，③「心理戦」，④「電子戦」，⑤「コンピュータ・ネットワーク戦」，⑥「実体破壊」と定義し，敵に対するレーダ

ー，通信妨害，錯乱による補足回避や電子パルスの照射による電子機器の破壊などによる「電子戦」と，コンピュータ・ウィルスの投入やハッキングによる敵の情報処理能力の破壊などの「コンピュータ・ネットワーク戦」とを同時連携して用いる「網電一体戦」を提唱している．また，「コンピュータ・ネットワーク戦」とは，「コンピュータ・ネットワーク攻撃」と「コンピュータ・ネットワーク防御」・「コンピュータ・ネットワーク偵察」が含まれているとしている[31].

本研究では，人民解放軍が，先ほどの戴清民のサイバー戦の定義に則って組織体制を構築しているものと仮定した上で，その組織詳細や任務などについて検証する．

(1) 正規部隊

ここからは，人民解放軍がいかなる組織陣容でサイバー戦の任にあたっているのかを確認しておきたい．

2011 年 5 月 25 日，中国国防部の耿雁生報道官は，国防部の定例記者会見において，広東省広州軍区にサイバー軍を創設したことに関して質問を受け，「部隊のインターネットセキュリティーの水準を向上させることが目的だ」と説明し[32]，人民解放軍の正規部隊としてサイバー部隊が存在することを認めた．同会見において耿報道官は，その目的に関しては，攻撃目的ではなくあくまでも組織防衛的な理由である旨を強調したが，同年 7 月の中国のテレビ番組の中で，人民解放軍が米国の大学に設置されていた法輪功関係のサーバーに攻撃を仕掛ける様子が実演された[33].

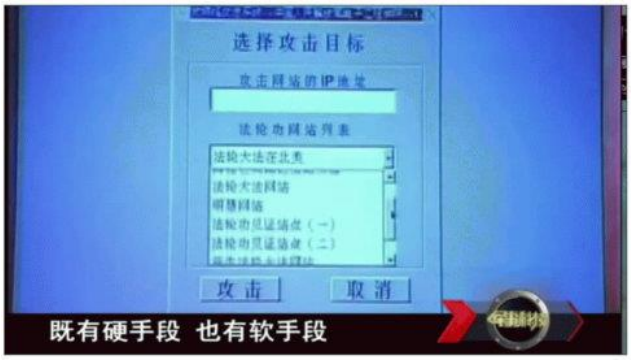

図 2　法輪功関係のサーバーに攻撃を仕掛ける様子

この事実からも，人民解放軍の正規部隊は，2011 年 7 月時点で敵対勢力に対するサイバー攻撃能力を備えていたのと同時に，既にサイバー攻撃の実戦行為に着手していたことは明白である．

同攻撃などを主導したと考えられるのが，人民解放軍総参謀部電子対抗雷達部（第 4 部）である．同部は，敵軍のレーダー探索，周波数や波長に関するデータの収集を行う電子偵察や，収集したデータをもとに有事の際に敵軍の通信電子活動に妨害や欺瞞を行う「電子戦」・「コンピュータ・ネットワーク攻撃」を担当している．また，直属または各軍区などの電子対抗部隊を指導している．つまり，同部はサイバー戦におけるオフェンスを掌っていると考えられる．

その一方で，サイバー戦におけるディフェンスを掌っていると考えられるのが，人民解放軍総参謀部技術偵察部（第 3 部）である．同部は，無線通信傍受，暗号解読，軍用偵察衛星が獲得する情報の分析・解読などの技術的分析及び無線通信の安全確保・妨害対策を担当している．また，先ほどの電子対抗雷達部と同様に，直属または各軍区などの技術偵察部隊を指導している．同部の組織任務から推察すると，同部は，サイバー戦においては「コンピュータ・ネットワーク防御」と「コンピュータ・ネットワーク偵察」を担当するとみられる．

この様に，人民解放軍は，サイバー空間における優位性獲得に照準を合わせ，総参謀部電子対抗雷達部と総参謀部技術偵察部という 2 つの正規部隊組織を編成し，その各々に攻撃と防御を分担させることで，サイバー戦の攻防一体戦略を意味する「網電一体戦」という，人民解放軍の最新の軍事戦略を具体化させていると考えられる．

これに加えて人民解放軍は，2010 年 7 月に，上述した両組織に加えて「総参謀部信息保障基地」を設立している．

図 3　総参謀部信息保障基地の設立式典の様子

設立時の報道によれば，同基地は胡錦濤・中央軍事委員会主席（当時）の軍事戦略を具現化し，軍の情報化の科学的発展に寄与するものとして設立されたと紹介されている[34]．同報道から推察するに，同基地は，従来からの総参謀部電子対抗雷達部と参謀部技術偵察部という攻守を分担して受け持つ 2 組織の機能の現代化を補完するため，指揮命令系統の統一性確保や人員・予算の効率的配分などを意図して組織横断的に新設されたと考えられるが，各種公然情報からは，同基地の実際の活動状況の詳細は把握できない．

(2) 民兵

本章の冒頭で指摘したように，中華人民共和国国防法第 22 条によれば，中国の軍事力には，人民解放軍現役部隊（正

規部隊と予備役部隊）に加え，民兵組織が含まれると規定されている[35]．では，サイバー戦において民兵は，いかに組織化され，また，いかなる任務を帯びているのであろうか．本研究の主たる目的である，「人民解放軍のサイバー戦における民間能力活用」と密接に関連するこのテーマについて，ここから検証していきたい．

人民解放軍は，1988 年ころから中国各地で情報技術の民間企業や研究機関などから人材を集めて，「民兵信息作戦分隊」を設立している．例えば，2004 年 5 月 18 日には，海南大学旅遊学院において，民兵信息作戦分隊である「海南省海口市美蘭区民兵信息戦連」の成立式が開催された．これには，海南大学信息学院の教員 4 名と 26 名の学生が参加しており，サイバー戦に有益な専門知識を有する現役の教職員が，人民解放軍の民兵として正式に組織化されたことが確認できる[36]．

図 4　「海南省海口市美蘭区民兵信息戦連」成立式の様子

2006 年にはサイバー戦における民兵組織設立戦略が明示的に打ち出されたが，それよりも以前の 2005 年，広州軍区の人民武装部は，彼らが利用できる人的資源を把握するとともに，民兵部隊や民間動員演習への参加の増大を促進するため，それぞれの地域における情報技術者の調査・登録を始めている．その成果を受け，従来は歩兵中心である民兵の徴募を農村部で行っていたのとは対照的に，サイバー戦において有益となる情報技術者などの徴募は都市部において行われるようになった[37]．

なお，各地方の主に都市部に所在する研究所，大学，情報産業などの情報技術者らを採用するのは民兵に限ったことではなく，人民解放軍の正規部隊，すなわち，総参謀部電子対抗雷達部や参謀部技術偵察部などでも彼らを採用することで民間能力活用を積極的に図っており，その有効性に対する内部評価も高いものがある[38]．

(3) 組織外協力者

ここまでは，人民解放軍の正規部隊と民兵という 2 つの組織について考察してきた．しかし，人民解放軍がサイバー戦に向けて組織化しているのは，正規部隊や民兵といった，いわゆる「正式な戦力」だけではない．いわゆる「愛国ハッカー」である純粋な民間人を組織外協力者として位置づけ，彼らの有する高度な情報技術を活用していることが窺われる．紙幅の関係で多くの事例を検証することはできないが，ここでは，自身も愛国ハッカーであり，ハッカー・グループ「Javaphile」の創設者である彭一楠を取り上げたい．

「Javaphile」は，2000 年に彭一楠によって設立されたが，同組織は，2001 年に海南島付近の南シナ海上空で米軍の電子偵察機と人民解放軍空軍の戦闘機が空中衝突した事件を受け，2001 年から 2002 年にかけてのホワイトハウスへのハッカー攻撃を敢行したことで知られる．このハッカー攻撃の後，彭一楠は何らの罪に問われることなく，逆に上海市公安局情報セキュリティ顧問に就任したことが確認されている[39]．さらに彼は，2008 年に，上海交通大学信息安全工程学院の研究会員名義で情報セキュリティ関連の論文を発表しているのだが[40]，同学院は人民解放軍のサイバー部隊である「61398 部隊」と共同研究を行うなど密接な関係を持っていることが判明している[41]．よって，愛国ハッカーとして米国にサイバー攻撃を実行した彭一楠と人民解放軍とは，組織外の協力関係者として密接な関係にあることが強く推察される．

4. 考察と提言

ここまで検証してきたように，人民解放軍は，①総参謀部内に正規のサイバー部隊を設け都市部での要員募集をおこなっているほか，②民兵として有力大学や情報産業に勤務する民間人を組織化し，さらにそれに加え，③愛国心を有し，党・政府に協力的な姿勢を示す民間ハッカーを組織外協力者として指導下におくなど，民間能力活用のレベルは極めて高いと言える．

これは，サイバー戦が，従来の陸・海・空を舞台にした戦闘行為とは異なり，最新技術によって成立するサイバー空間という仮想世界での戦闘行為であることから，あえてすべての人的資源を人民解放軍内に常時取り込んでおく必要がないことや，サイバー攻撃の際に発信元などを高度に隠ぺい，あるいは，少なくとも人民解放軍施設内からの攻撃ではないと強弁するための防衛策と考えられる．

米国のサイバー戦における中国に対するアプローチを，対抗戦力の確保と国際秩序枠組みへの取り込みとを並行する「硬軟二段構えの対中戦略」と称する意見[42]があるが，では，我が国は一体，いかなる方策を持って，人民解放軍が着々と進めるサイバー戦に向けた民間能力活用に対抗すべきなのであろうか．この点に関しては，国民的議論はおろか，政治ないし行政の領域でも未だ明確な方針は定まっていないように思われる．

そこで本研究では，「内」と「外」の観点から，次の 2 点を提言したい．

一つ目は「内」であるが，サイバー戦に向けた法的整備と民間能力活用の推進である．我が国の現行法によれば，自衛隊が自衛権の範囲内としてサイバー空間における正当な反撃行為を行うことに関して，罰則の例外規定を設けた条項は存在しない．したがって，相手国からのサイバー攻撃に反撃する行為は，現状，不正アクセス行為の禁止等に関する法律[43]や電子計算機損壊等業務妨害罪[44]に該当する違法行為となる蓋然性が極めて高い．サイバー戦における自衛権については，さまざまな意見や議論の余地があろうが，いずれにしても早急なる対処が求められる．さらに，人民解放軍が民兵や組織外協力者を確保・組織化している現状を鑑み，我が国においても平素の内から，サイバー戦に関する情報交換など常時行う官民協力体制を構築しておくこと，すなわち民間能力の集約化が必要である．

「外」となる二つ目は，我が国が主導して国際的なルール作りを目指すことである．我が国を含め，現在，米国や EU など世界 30 カ国が批准するサイバー犯罪条約は，コンピュータシステムという手段によって行われるすべての犯罪が対象とされているなど，その適用範囲は極めて広い．同条約によれば，加盟国はサイバー犯罪に対処するための刑事手続きを含めた法的整備や犯罪人引き渡しや捜査への共助規定を設けるなどし，同犯罪の防止や検挙に資することになっている．しかし，中国は同条約に加盟しておらず，人民解放軍のサイバー部隊や民兵組織による加害行為を他国がある程度特定したとしても，中国に対して何らかの対処を求める法的根拠は存在しない．すなわち，高い能力を有する人民解放軍や軍外協力者によるサイバー攻撃などを規制する法的要因は存在しないこととなる．よって，まずはこの現状の改善が求められるだろう．

さらに必要なのが，ジュネーブ条約やハーグ条約のような戦時規定を盛り込んだ，サイバー空間に適用される新たな国際法の整備である．冒頭でも紹介したように，すでにサイバー空間は「第 5 の戦場」と認識されている．それであるのにも関わらず，サイバー空間には，ROE（Rules of Engagement：交戦規定）や戦時規定が存在しないだけでなく，先ほど述べたように通常の犯罪行為の抑止を図る国際条約ですら，わずか 30 数カ国程度の加盟国にしか影響力を及ぼさない．この状況は，極めて危険ではなかろうか．事実上，既にサイバー空間は多くの国の軍隊などがせめぎ合う戦闘空間なのであるから，例えそこが不可視であっても，戦場として成立する空間であることを世界各国が認め合い，新たな規律・規範を設けることが必要であろう．

確かに，2013 年 6 月には，日本など主要 15 カ国が参加する国連の政府専門家会合が「国連サイバー安保報告書」をまとめ，サイバー空間にも既存の国際法，特に国連憲章が適用されるべきだと勧告し，同時に，攻撃者の特定が難しく疑心暗鬼を生じやすいというサイバー攻撃の特性を鑑み，信頼醸成の重要性が指摘された[45].

また，2013 年 3 月には，NATO（North Atlantic Treaty Organisation：北大西洋条約機構）が，いわゆる「タリン・マニュアル（The Tallinn Manual)」を作成した．しかしながら，これらはガイドラインの域を脱していない．我が国が率先して，「国連サイバー安保報告書」や「タリン・マニュアル」などをベースに，より具体化，かつ実行力を伴う新たな国際法の制定に向けた世界的な機運を盛り上げていくことが肝要である．それこそが平和主義と専守防衛を国是に掲げる我が国の責務ではなかろうか．

5. おわりに

ここまで検証してきたように，新たな戦争形態としてのサイバー戦に対処するため，人民解放軍は，あらゆる民間能力を集約し，その活用を図っている．常に外敵への危機意識を持ち国家をあげて対処を図るという，その貪欲なまでの姿勢は，我が国も参考にすべき面があるのではないか．本研究は，サイバー戦に対する我が国の危機管理への啓発的意味合いを込めて着手したという側面もある．

社会的環境の変化に敏感で，時として予想外なほどに柔軟な対応を見せる人民解放軍の動向を把握し続けることは容易いことではないが，今後も本研究を深化させていきたいと考えている．

参考文献

1）伊東寛『「第 5 の戦場」サイバー戦の脅威』，祥伝社，2012 年，p.33
2）『朝日新聞』2000 年 2 月 25 日朝刊
3）『朝日新聞』2006 年 2 月 5 日朝刊
4）『朝日新聞』2007 年 9 月 5 日夕刊
5）『朝日新聞』2008 年 3 月 4 日夕刊
6）『朝日新聞』2009 年 4 月 23 日朝刊
7）『朝日新聞』2010 年 1 月 16 日夕刊
8）『朝日新聞』2010 年 2 月 20 日夕刊
9）『読売新聞』2011 年 10 月 4 日朝刊
10）『朝日新聞』2011 年 11 月 7 日朝刊
11）『朝日新聞』2012 年 9 月 20 日朝刊
12）『読売新聞』2012 年 11 月 8 日夕刊
13）『読売新聞』2013 年 2 月 21 日朝刊
14）『朝日新聞』2013 年 3 月 15 日朝刊
15）『ロイター社』ウェブサイト
http://jp.reuters.com/article/topNews/idJPTYE91I03620130219
（2013 年 10 月 2 日閲覧）
16）杉山徹宗『軍事帝国中国の最終目的』，祥伝社，2005 年，pp118-119.
17） 富坂聰『中国人民解放軍の内幕』, 文春新書, 2012 年, pp82-85.
18）塩沢栄一『中国人民解放軍の実力』，ちくま新書，2012 年，pp.134-135.
19）平松茂雄『中国人民解放軍』，岩波新書，1987 年，p.49
20）同上書，p.171
21）『解放軍報』，1997 年 9 月 14 日付
22）矢吹晋『中国人民解放軍』，講談社，1996 年，p.173

23）劉華清「堅定不移地沿着建設有中国特色現代化軍隊的道路前進」『求是』1993 年第一五期 8 月 1 日付
24）「中共中央政治局第 15 次集体学习 主題为国防建设」『中国新聞網ウェブサイト』
http://news.sohu.com/20040724/n221179200.shtml
（2013 年 9 月 30 日閲覧）
25) 浅野亮「軍事ドクトリンの変容と展開」, 村井友秀, 阿部純一, 浅野亮，安田淳編著『中国をめぐる安全保障』，ミネルヴァ書房，2007 年，p.279
26）『中国共産党第 17 回全国代表大会ウェブサイト』
http://www.peopleschina.com/maindoc/html/17da/index.html
（2013 年 10 月 3 日閲覧）
27）金千里『解放軍現役将領評伝』，夏菲爾出版有限公司，2010 年
28）国務院新聞弁公室『2010 年中国的国防』中華人民共和国中央人民政府網
http://www.gov.cn/jrzg/2009-01/20/content_1210075.htm
（2013 年 10 月 2 日閲覧）
29）『中国共産党第十八回全国代表大会ウェブサイト』など
http://jp.xinhuanet.com/zt/18cpcnc/
（2013 年 10 月 3 日閲覧）
30）『Bloomberg ウェブサイト』
http://www.bloomberg.co.jp/news/123-MO4ARB6TTDSA01.html
（2013 年 10 月 3 日閲覧）
31）『解放軍報』2003 年 7 月 1 日付
32）『新華社ウェブサイト』
http://www.xinhua.jp/socioeconomy/politics_economics_society/275438/
（2013 年 9 月 25 日閲覧）
33）土屋大洋『サイバー・テロ 日米 vs.中国』，文藝春秋，2012 年，p.86
34）「陈炳德出席信息保障基地成立大会并授军旗」『人民網ウェブサイト』
http://military.people.com.cn/GB/172467/12193636.html
（2013 年 10 月 1 日閲覧）
35）『中国人民代表大会ウェブサイト』
http://www.npc.gov.cn/wxzl/gongbao/2000-12/05/content_5004681.htm（2013 年 9 月 20 日閲覧）
36）「海南省第一个高校学生民兵组织在海南大学成立」『海南大学武装部ウェブサイト』
http://www.hainu.edu.cn/stm/zy_wuzhuangbu/2004519/1591.shtml
（2013 年 10 月 3 日閲覧）
37）Bryan Krekel, Patton Adams, George Bakos, *Occupying the Information High Ground : Chinese Capabilities for Computer Network Operations and Cyber Espionage*, U.S.-China Economic and Security Review, March 7,2012
38） 李軍「挖掘地方高科技资源推进民兵信息化建设」『国防』, 2004 年，9 号
39）「美智库称网络安全全赖中国」『多維新聞ウェブサイト』
http://national.dwnews.com/news/2013-03-14/59155523.html
（2013 年 10 月 4 日閲覧）
40） 彭一楠「浅析 SQL 盲注攻击的实现」『信息安全与通信保密』, 上海交通大学信息安全工程学院，2008 年，5 号
41）『REUTERS CANADA ウェブサイト』
http://ca.reuters.com/article/topNews/idCABRE92N01120130324
（2013 年 10 月 4 日閲覧）
42）谷口長世『サイバー時代の戦争』，岩波書店，2012 年，p.151
43）平成 11 年 8 月 13 日法律第 128 号
44）刑法第 234 条第 2 項
45）『読売新聞』2013 年 10 月 5 日付朝刊