ハイブリッド戦争をめぐる諸外国の政策と動向

國　吉　孝　志

目　　次

はじめに
1．米国の対テロ法制と諜報活動
（1）米国のテロ対策
（2）西欧諸国への影響
2．「ハイブリッド戦争」と米国のサイバー戦略
（1）ロシアによるウクライナ侵攻
（2）2016年アメリカ大統領選挙への干渉疑惑
（3）中国版「ハイブリッド戦争」の展開
（4）米国のサイバー戦略
3．ドイツの「SNS法」とNATOの危機感
（1）ポピュリスト政党の台頭
（2）ドイツ「SNS法」
（3）欧州要人の意識変化
（4）米国との連携の動き
4．「タリンマニュアル2.0」
5．我が国の法整備の現状
（1）サイバーセキュリティ基本法
（2）我が国の安全保障政策の転換
（3）通商・金融分野へ拡大する安全保障政策
おわりに

はじめに

近年、安全保障政策においてサイバー空間に関する議論が活発である。我が国においても「平成31年度以降に係る防衛計画の大綱について（30大綱）」とともに策定された「中期防衛力整備計画（2019）」では、「多次元統合防衛力」の構築が明記され、従来の防衛力強化に加えサイバー防衛力強化が推進された。それほどに現在では軍事と非軍事の境界が曖昧となり、サイバー防衛といっても防衛の対象は軍事施設、防衛産業、社会インフラ、民間の経済活動をはじめとする一般社会全般へと広がり、民主主義国家においては、自由な価値観や思想に基づく表現や主権の正当性を担保する選挙制度ですら脅威にさらされているのが実情である。われわれの身近な生活は、IoT化された多数の電化製品、情報通信機器、ハイテク製品に支えられ、その規模や範囲は今後も発展していくことは確実である。それと同時にサイバー空間における脅威はより複雑化し広範囲なものとなっている。サイバー防衛に関しては、現代の情報通信技術の進展以前から軍事・非軍事組織を問わず情報戦、心理戦、諜報といった活動がそれぞれの国家の国益を守り、常に戦争遂行能力にも内包されていた。国民は第二次世界大戦以降もメディアを通して戦場を目の当たりにし、メディアがその戦争の是非についての国民世論の形成に影響をあたえるため、各国政府は戦略的にメディアの報道を無視することができないのはその一例である。しかしながらインターネットが普及した今日では、個人のラットトップ、スマートフォンからリアルタイムでインタラクティブに情報が交換され、SNS（ソーシャル・ネットワーキング・サービス）による個人の情報発信が世界中で行われている。これは戦略的価値を持つメディアの活動が個人レベルで容易になったことを意味しており、各国の安全保障政策においても大きな転換期となるものである。2001年９月11日以降、アメリカをはじめとする世界各国はテロ対策を安全保障上の課題に取り上げ、西側諸国のみならず、ロシア、中国等もその対策に取り組んできた。我が国でも、防衛政策や警察行政においてテロ対策が中心的な課

題とされてきたことは事実である。そのなかでもサイバーインテリジェンスは対テロ政策の重要なオプションであり、事実、2001年の「米国愛国者法（USA PATORIOT Act）」等の立法政策やエドワード・スノーデンが暴露したNSA（National Security Agency）の電子的諜報活動（Signals intelligence）からも明白である。このような非対称戦を中心とした政策は大国間の戦略や関係性にも大きな影響を与えたといえる。現在のロシアが孤立する起因となったクリミア併合はサイバー攻撃を発端にオペレーションが遂行され、ロシアのサイバー攻撃は2016年のアメリカ大統領選挙介入疑惑事件という形で世界を震撼させた。中国はこれまでにもアメリカの軍事施設、軍需産業へのハッキング、サイバー攻撃を繰り返し、我が国へも不正なアクセスを試みてきた。このような軍事戦略は「ハイブリッド戦争（Hybrid warfare）」とよばれ、我が国を含めた各国の軍事関係者の議論の中心となっている。従来は、経済力、軍事力を構成するハードパワー（Hard power）と文化、価値観、生活様式を構成するソフトパワー（Soft power）が国際社会における影響力資源とされてきたが、2017年、「米シンクタンク全米民主主義基金（National Endowment for Democracy）」において新たに「シャープパワー（Sharp power）」という呼称が登場した。これは、権威主義国家による民主主義国家への情報歪曲や世論操作により影響力の優位性を図ったものであり、自由や権利といった民主主義国家の理念、正当性を根本から覆す脅威となる。

本稿では、諸外国の対テロ立法等を中心とした情報通信分野におけるテロ対策の動きを参考に、表現規制やプライバシーの問題として議論されてきた法制度についてその意義や特色について検証していく。

諸外国の法制度に関しては、各国の歴史的経緯、統治機構、憲法制度等によりさまざまであり、目的も執行のプロセスも一概に比較することは困難である。アメリカ合衆国では、冷戦期から自由主義陣営の盟主として、社会主義陣営の脅威に対峙してきた。しかし同時多発テロ以降では、2001年制定の「米国愛国者法（USA PATORIOT Act）」、2011年同法を延長した「愛国者法日没条項延

長法（PATORIOT Sunsets Extension Act of 2011）」が民主主義国家の価値観として議論の対象となった。「米国愛国者法」失効後の2015年には、情報監視活動について規定した「米国自由法（USA FREEDOM Act of 2015）」が制定された。2017年、トランプ政権は、「国家安全保障戦略（NATIONAL SECURITY STRATEGY）」を発表し、このなかでも中国、ロシアの脅威を強調している。アメリカの安全保障上の脅威とされる中国企業「ファーウェイ」等との取引を禁止する「米国国防権限法2019（NATIONAL DEFENCE AUTHORIZATION ACT FISCAL YEAR 2019）」はサイバー戦略において中国を深刻な脅威と捉えている証左である。ドイツ連邦共和国基本法（ボン基本法）では、「戦闘的民主主義」の概念で知られるとおり、基本法で保障される基本権は民主主義の価値を否定することに濫用することは許されない。このことはドイツが過激主義的な価値観から民主主義を守るという意味において果たしてきた役割は大きく、現代においても新しい課題に対応するべく議論が続けられている。また、ドイツの政治学者セバスチャン・ハイルマンは中国の共産党一党独裁体制を確立するためのデジタル技術の活用を「デジタル・レーニン主義（Digital Leninism）」と名づけ、新しい社会管理システムの構築を進める中国の現状を説明した。NATOにおいては、ロシアの「ハイブリッド戦争」の脅威に直面しており、エストニアの首都タリンでサイバー攻撃へ対抗するための国際法適用の研究成果をまとめた「タリンマニュアル2.0（Tallinn Manual2.0）」を2017年に発刊した。サイバー攻撃に対し、国際法上軍事力で対抗することを想定した場合、このような研究は我が国のサイバー防衛を検討する上でも今後の進展が注目される。

「ハイブリッド戦争」に関する研究や議論は、このように欧米の政治や安全保障政策の動向が注目されるものの、アジア地域においてもその脅威は日々増しているのが現状である。台湾では海峡を挟んだ中国と政治的、軍事的な対立が継続しており、香港でも2019年のデモのさなか中国当局の動きは活発であった。諸外国の政策や動向は今後我が国が「サイバー防衛力」を構築し、実際の政策や法的諸問題に対処する上でも重要な指針となるため、多角的に検証したい。

１．米国の対テロ法制と諜報活動

（１）米国のテロ対策

アメリカに対する大規模なテロは1998年８月７日のケニアとタンザニアにおけるアメリカ大使館爆破事件、2000年10月12日イエメンアデン港においてはミサイル駆逐艦コール襲撃事件等、複数の事件が発生しているが、全世界に最も大きなインパクトを与えたのは2001年９月11日に発生した「アメリカ同時多発テロ事件」（以下、同時多発テロ）であることは明白であろう。この事件以降、アメリカでは国家戦略の大幅な転換が進められ、「対テロ戦争」と称する米軍の軍事行動が世界規模で展開されるに至った。このような状況は、国際情勢が流動化する現在においても継続しており、テロ対策の重要性は一貫したものであるといえる。ただ、この同時多発テロが、アメリカの立法政策にも大きな影響を及ぼしたことは事実である。まず、アメリカ国内でのテロ防止、テロ発生時の対処を目標とし、2002年７月16日に発表された「米国国土安全保障戦略（THE NATIONAL STRATEGY FOR HOMELAND SECURITY）」において、「テロ対策の目的を達成するために連邦レベルで法律を作成することは必要ではあるが、我々は新しく作成される連邦法が州法を不必要に先占したり、テロ対策を過度に連邦化したりしないことを保証するよう慎重に行動しなければならない。合衆国憲法第10修正は、州が、公衆の一般的な福祉について独立した権限を有することを明示しているのである。」(1)と連邦法と州や自治体の立法権に

(1) 中川かおり「主要国における緊急事態への対処：総合調査報告書　Ⅳ　テロ対策　1　アメリカ」、国立国会図書館調査及び立法考査局、国立国会図書館（2003）72頁。
「米国国土安全保障戦略」での原文は以下の通りである。
Where new legislation at the federal level is necessary to accomplish our counterterrorism goals, we should work carefully to ensure that newly crafted federal laws do not preempt state law unnecessarily or overly federalize counterterrorism efforts. The Tenth Amendment makes clear that each state retains substantial independent power with respect to the general welfare of its populace.
“THE NATIONAL STRATEGY FOR HOMELAND SECURITY” (2002) p.47.

配慮した形でその方針が示された。

同時多発テロ以降制定された連邦法は多数あるが、なかでも注目するべきものは2001年の「米国愛国者法（USA PATORIOT Act）」（以下、愛国者法）である。同法は、法執行機関の捜査情報収集の権限強化（201条）と諜報機関等への開示（203条）、テロリストのマネーロンダリング対策（311条、312条、319条）、テロとの関係が疑われる人物の強制退去や拘束の権限の強化（412条）が定められるなど(2)、広範囲な合衆国法典の改正と条文が規定された。特に第213条の、捜査への危険を防ぐために捜査官が令状の通知なしに家宅等を捜査できることを定めた規定については、不当な逮捕・捜査・押収の禁止を定めた合衆国憲法第４修正の趣旨に反するおそれがあることから、人権保障上の議論にもなったものである(3)。この法律は、第１章から第10章で構成され、なかでも電子的諜報活動に関する規定については第２章の201条に「テロリズムに関連する有線通信、口頭の会話及び電子的通信を傍受する権限」が、202条に「コンピュータ詐欺及びコンピュータ濫用罪に関連する有線通信、口頭の会話及び電子的通信を傍受する権限」が規定されており(4)、第10章雑則の1003条では217条で規定される「不正アクセス者の行う通信の傍受」との関係から、「第217条の規定に基づき､不正アクセス者を監視するための通信傍受が合法化されることに伴い、その種の通信傍受が外国諜報監視法にいう電子監視に該当しないことを、定義の一部を改めることにより明確にする」として「電子監視」の定義が規定された(5)。また、1978年成立の「外国諜報監視法（Foreign Intelligence Surveillance Act）」（以下、FISA）との関連として、愛国者法の通信監視活動に

---

(2) “UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001” PUBLIC LAW 107-56—OCT. 26, (2001)

(3) 平野美恵子、土屋恵司、中川かおり「米国愛国者法（反テロ法）（上）」、『外国の立法』214、国立国会図書館（2002）3-4頁。

(4) 平野美恵子、土屋恵司、中川かおり、前掲論文、17頁。

(5) 平野美恵子、土屋恵司、中川かおり、前掲論文、44頁。

関する各規定はこのFISAを改正するものである。その一例として、愛国者法218条の外国諜報情報の入手は捜査の「目的」として必要とされていたが、この要件が緩和され、「重要な目的の一つ」があれば別に主たる目的がある場合にもFISAに基づく外国諜報情報の入手が可能とされた。この条文は刑事捜査と外国諜報情報収集の境界をあいまいにしている(6)。その他、愛国者法の特徴として、複数の規定が時限規定とされている点である。224条では「時限規定」として、「監視手続の改善」について定めた第２章の規定を対象に、2005年12月31日に失効することが明記されている(7)。しかしその後、2005年７月に、愛国者法と「2004年の諜報改革およびテロ予防法（The Intelligence Reform and Terrorism Prevention Act of 2004）」の再承認が議会の両院で可決され延長された。その中で、テロリストの死刑、海港施設の警備の拡充、テロリストの経済活動に対する制裁として新たな措置、シークレットサービスの新たな権限、覚醒剤の取り締まりなど新たな条項がつくられた。また、2006年２月には愛国者法の追加再承認修正法が最初の修正法として可決された(8)。2009年12月31日の失効に際し、第２章の２つの条文を除きすべて再承認され、「1978年外国諜報監視法に基づく移動傍受」について規定した206条と、「外国諜報監視法に基づく記録及び他の情報の入手」について規定した215条は改正された(9)。そして2010年２月27日にバラク・オバマ大統領（以下、オバマ大統領）は、議論となった１．裁判所の承認を得た複数の電話の盗聴を許可、２．裁判所の承認を得た対テロ作戦における記録と財産の押収を許可、３．アメリカ人以外で、指定されるテロググループ以外の可能性がある、いわゆる「ローン・ウルフ型」のテロリストの監視を許可する３つの条文の一時的な１年間延長の法律に署名

(6) 鈴木滋、「米国自由法―米国における通信監視活動と人権への配慮―」、『外国の立法』26、国立国会図書館（2016）7-8頁。
(7) 平野美恵子、土屋恵司、中川かおり、前掲論文、20頁。
(8) “USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005” U.S. H.R.3199, Public Law 109-177 (2006)
(9) “FISA Sunsets Extension Act of 2011” U.S.H.R.514-112th Congress (2011-2012)

した(10)。2011年５月26日、オバマ大統領はオートペンを使用し、「愛国者法日没条項延長法（PATORIOT Sunsets Extension Act of 2011）」に署名した(11)。ここまでで愛国者法の制定から延長、修正の経緯の概略を確認したが、その後これらの法律に重大な影響を及ぼしたのが、NSA元職員のエドワード・スノーデン（Edward Snowden）が、米国の情報収集活動に係る大量の機密文書をリークし、イギリスの「ガーディアン」がスクープした2013年の「スノーデン事件」である(12)。この事件でスノーデンが明らかにしたのは、NSA（National Security Agency）（以下、NSA）が「プリズム（PRISM）」というコードネームを付与されたプログラムを活用し、FBI（Federal Bureau of Investigation）（以下、FBI）が愛国者法215条を根拠に、外国諜報活動再審裁判所（United States Foreign Intelligence Surveillance Court）（以下、FISC）に対し、電話会社へのデータ提出命令の承認を求め、毎日継続的に提出されたデータを、NSAのデータベースに取り込む形で収集していたというものであった(13)。このことはテロ対策を目的とするアメリカ市民のプライバシーの扱いや、FISCの改革、愛国者法215条の問題点などについて大きな議論を呼んだ。2015年には愛国者法215条やFISAの期限切れを迎えるにあたり、通信監視活動の改善を図る動きが活発となり、紆余曲折はあったものの、４月28日に「2015年米国自由法」として提出された二つの法案のうち、下院法案第2048号（H.R.2048）が最終的に６月２日に上院を通過後、オバマ大統領の署名を経て「2015年米国自由法（USA FREEDOM Act of 2015）」が新たに成立した(14)。本法律は第１章から第７章

⑽ Julie. Kent, “Obama signs one year extension of Patriot Act” Entertainment Archives (2. 28, 2010)
https://web.archive.org/web/20101121121929/http://clevelandleader.com/node/13183（2020年４月22日閲覧）

⑾ “Obama Signs Last-Minute Patriot Act Extension” Fox News (5. 27, 2011)
https://www.foxnews.com/politics/obama-signs-last-minute-patriot-act-extension（2020年４月22日閲覧）

⑿ 鈴木滋、前掲論文、９頁。

⒀ 鈴木滋、前掲論文、９頁。

⒁ 鈴木滋、前掲論文、12-13頁。

で構成され、第２章201条「大量収集の禁止（FISCへの通信監視活動承認の請求）」、第３章301条「違法に入手した情報の使用制限」、第４章401条「法廷助言者の指名」第５章501条「大量収集の禁止（捜査機関の通信記録提出命令の請求）」等からも愛国者法の反省を踏まえたものとなっている(15)。

（２）西欧諸国への影響

以上がアメリカ同時多発テロ以降の電子的諜報活動を中心としたアメリカのテロ対策の軌跡であるが、他の西側諸国においても同様の動きがみられる。フランスでは、インターネットに関する規制について、刑法を中心とした各種法令が存在するが、インターネットの影響を受けた国民のシリア・イラク地域への渡航増加を受け、2014年、「テロリズムの対策に関する措置を強化する2014年11月13日旧法第2014-1353号」（以下、2014年テロ対策法）が制定され(16)、同法では第５条において「テロ扇動罪」、「テロ称賛罪」を刑法典に移し罰則を強化した。また、第６条では、刑事訴訟法典706-23条の改正によりインターネットを介したテロ行為の扇動・称賛による明白で違法な混乱がある場合、検察官、訴えの利益がある自然人、法人の訴えを受け、裁判官はインターネットサービスの停止命令が可能となった(17)。ドイツでは連邦刑事警察庁のテロ調査権限について、2009年に施行された連邦刑事警察庁法（Bundeskriminalamtgesetz）の改正により、国際テロ防止のため、住居内の録音録画や、オンライン捜索等の監視措置を当事者への告知なしで行う権限を得た(18)。2016年４月20日、連

⑮ “UNITING AND STRENGTHENING AMERICA BY FULFILLING RIGHTS AND ENSURING EFFECTIVE DISCIPLINE OVER MONITORING ACT OF 2015” U.S. H.R. 2048, PUBLIC LAW 114-23 (2015)

⑯ 大沢秀介、新井誠、横大道聡　編著、『変容するテロリズムと法―各国における〈自由と安全〉法制の動向』、弘文堂（2017）128頁。

⑰ 大沢秀介、新井誠、横大道聡　編著、前掲書、（2017）129頁。

⑱ 大沢秀介、新井誠、横大道聡　編著、前掲書、（2017）146頁。

邦憲法裁判所（Bundesverfassungsgericht）は、連邦刑事警察庁への監視措置の権限付与の合憲性は認めつつも、１．具体的な事件が予見されることや具体的な蓋然性を要件とし、２．収集したデータの他官庁への伝達は急迫性がある場合に限られ、一般的なテロ防止のためのデータ伝達は違憲であるとした(19)。また、前述のスノーデン事件はドイツにも影響を与えており、ドイツ連邦情報局（Bundesnachrichtendienst）の米国NSAへの情報提供が問題となり、2016年に連邦情報局法（BND法）が改正された(20)。これはスノーデン事件をきっかけに法律の根拠の明確化を図ったものであり、「通信情報収集の目的」、「通信情報収集の対象」、「通信情報収集の方法」、「連邦首相府の命令」、「外国の諜報機関との協力」、「統制」について規定された第２章が新設された(21)。

このようにアメリカ同時多発テロはアメリカとその同盟国のテロ対策や立法政策の大きな転換期であったことがわかる。「対テロ戦争」の特徴として、国際条約に基づく正規軍同士の戦争形態とは異なる非対称戦（Asymmetric war）があげられるが、その中で電子的諜報活動は大きな役割を果たし、一方でサイバー空間はISIS等にみられるように国際テロ組織のプロパガンダの温床にもなった。このことは、国家間の対立やインテリジェンスにおいても「ハイブリッド戦争」という形で拡大したといえる。後述するロシアによる2014年クリミア危機、2016年アメリカ合衆国大統領選挙への干渉疑惑はその例であり、「対テロ戦争」のリニューアル版ともいえる動きととらえることもできる。

⑲　大沢秀介、新井誠、横大道聡　編著、前掲書、（2017）146-147頁。
⑳　大沢秀介、新井誠、横大道聡　編著、前掲書、（2017）150頁。
㉑　大沢秀介、新井誠、横大道聡　編著、前掲書、（2017）150-151頁。

2．「ハイブリッド戦争」と米国のサイバー戦略

（1）ロシアによるウクライナ侵攻

「ハイブリッド戦争（Hybrid warfare）」という名称が西側メディアに取り上げられるようになったのは、2014年にロシア軍によるクリミア半島、ドンバス地方への侵入、住民を扇動したうえでウクライナからの分離・独立を成功させた事件である[22]。このオペレーションでは、ロシア軍の空挺部隊（VDV）、特殊作戦群（SSO）の他、非正規軍の支援要員までも動員し、さらにロシア連邦保安庁（FSB）の支援を受けた民兵集団によるウクライナ治安機関への襲撃、各種ロシア軍装備品の提供や、ロシア兵によるものも含むSNS（ソーシャル・ネットワーキング・サービス）への投稿などの軍事活動が行われた[23]。ロシア軍参謀総長ゲラシモフ（Valery Gerasimov）によれば、「アラブの春」を念頭に、21世紀の戦争は古典的な戦争の形式や手順に当てはまらない政治、経済、情報、人道問題とその他幅広い「非軍事手段」が主となることを示唆している[24]。NATO議会会議・市民安全保障委員会（Committee on the Civil Dimension of Security）の報告書によると、他国への政治介入、スパイ活動、犯罪行為、虚偽情報（Disinformation）、プロパガンダ、サイバー攻撃等も「ハイブリッド戦争」に活用される非軍事的な有効手段とされる[25]。前述のとおり、このウクライナでの「ハイブリッド戦争」では、ロシア軍の特殊部隊の支援を受けた親ロシア派の武装とともに暴力行為が発生し、虚偽情報や陰謀論がソーシャルメディ

---

(22) 小泉悠、「ウクライナ危機にみるロシアの介入戦略　ハイブリッド戦争とはなにか」、『国際問題』No.658、国際問題研究所（2017）40頁。
(23) 小泉悠、前掲論文、44頁。
(24) 小泉悠、前掲論文、41-42頁。
(25) 志田淳二郎、「クリミア併合後の『ハイブリッド戦争』の展開―モンテネグロ、マケドニア、ハンガリーの諸事例を手がかりに」、「国際安全保障」第47巻第4号、国際安全保障学会（2020）22頁。

アやロシア政府系メディア「RTネットワーク」により拡散され、国籍を秘匿したロシア軍部隊がウクライナに侵入するというプロセスで行われているが(26)、当時のNATOアメリカ政府代表のアイヴォ・ダールダーによれば、「これは、要するに、従来の軍事進攻ではなかった。何が起きているのか敵が理解すらしないうちに目的が達成されるハイブリッド戦だった」と振り返り、NATO欧州連合軍最高司令官フィリップ・ブロードラヴは、「情報戦史上最も驚異的な情報の電撃戦」と評している(27)。

（2）2016年アメリカ大統領選挙への干渉疑惑

ロシアが関わったとされるこのような情報戦は局地的な軍事行動に限定されたものではなく、対象国に対する世論誘導や選挙への干渉、介入といった形でその脅威は高まっている。2015年に民主党全国委員会（Democratic National Committee）（以下、DNC）がロシアの諜報機関の関与によるハッキングを受け、ヒラリー・クリントン候補にとって不利となる電子メール情報が流出し、選挙中にFBIまでもが調査に乗り出す事態に発展したことは当時世界中で大きく報じられた。このことについて、前述の「2004年の諜報改革およびテロ予防法」により設置されたアメリカのインテリジェンス・コミュニティを統括する国家情報長官室（Office of the Director of National Intelligence）（以下、ODNI）は2017年に「最近のアメリカ合衆国におけるロシアの活動と意図の評価」において背景を含む詳細な報告書をまとめている。この報告書によると、この2016年アメリカ大統領選挙への影響を狙った作戦はウラジミール・プーチン大統領の命令のもとで行われ、アメリカの民主主義に対する国民の信頼を失墜させ、当時有力とされたヒラリー・クリントン長官を侮辱し、大統領選出の可能性を

---

(26)　P.W.シンガー、エマーソン.T.ブルッキング　著、小林由香利　訳『「いいね！」戦争　兵器化するソーシャルメディア』NHK出版（2019）324-325頁。
(27)　P.W.シンガー、エマーソン.T.ブルッキング、前掲書、326頁。

害することで、比較的プーチン大統領とロシア政府に好意的なドナルド・トランプの選出を望むものであった。プーチン大統領はパナマ文書の公開やオリンピックにおけるドーピング問題でロシアが中傷を受けたこと、2011年後半から2012年初頭にクリントン長官から公然と体制批判を受けたことに対する怨嗟なども動機につながったとされる。この報告書においても、背景として、前述のウクライナにおける作戦から、ロシアの「ハイブリッド戦争」の側面についても触れられている[28]。また、報告書によると、2016年３月までにロシア連邦軍参謀本部情報総局（以下、GRU）主導でこのオペレーションは開始され、民主党役員や政治家のEメールアカウントを収集し、５月までにはDNCから大量のデータを流出させた。GRUはルーマニア人ハッカー「グシファー2.0（Gussifer2.0）」を名乗り犯行に及んだ上、ジュリアン・アサンジ（Julian Paul Assange）を創始者とする「ウィキリークス（WikiLeaks）」を利用して暴露した。アサンジについては、2013年８月、前述のロシア国営メディアRTの編集長とロンドンのエクアドル大使館において放送契約のために面会していることも明らかにされている。ロシアにはこのRTに加え、「スプートニク（SPUTNIK）」というメディアも存在し、両社はロシア政府のプロパガンダに貢献してきた[29]。2016年の大統領選挙だけでなく、これまでにも2012年のオバマ大統領の再選の際にもロシア政府により創設され出資を受ける「RTアメリカ」によるプロパガンダが行われていたことも明らかにされている[30]。

---

[28] “Russia’s Influence Campaign Targeting the 2016 US Presidential Election” Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution Office of the Director of National Intelligence (2017) pp.1–2.

[29] “Russia’s Influence Campaign Targeting the 2016 US Presidential Election” Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution Office of the Director of National Intelligence (2017) pp.2–4.

[30] “Russia’s Influence Campaign Targeting the 2016 US Presidential Election” Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution Office of the Director of National Intelligence (2017) p.6.

（３）中国版「ハイブリッド戦争」の展開

サイバー空間における諜報活動やプロパガンダを活発に行っているのは、中国も同様である。2010年代に入り、中国のサイバー攻撃をアメリカは非難し、FBIは中国人民解放軍（以下PLA）のサイバー戦部隊の関係者の起訴、指名手配を行っており、最近の例では2020年１月28日、ジョージア州北部地域の大陪審においてPLAの第54研究所のメンバー４名を、コンピュータ詐欺、産業スパイ、通信詐欺、コンピュータ詐欺の共謀、産業スパイ実行の陰謀および通信詐欺の陰謀等の罪状で起訴した。犯行の概要は2017年５月13日または７月30日前後にアメリカ政府機関のコンピュータへ不正アクセスし、約１億4500万人のアメリカ国民の生年月日と社会保障番号、1000万人の運転免許証番号、その他クレジットカード番号と20万人のアメリカ人の個人が特定できる情報を入手したとされている(31)。また、ロシア同様、世論誘導や政治介入の例もある。2018年の台湾統一地方選挙では、高雄市の市長として韓國瑜が勝利し、その後半年で、2020年１月の総統選に向けた最大野党・国民党の予備選にまで乗り出した。国民党の公認を受けた韓は急進的に支持率を伸ばし民進党の牙城ともいうべき高雄市長の座を勝ち取ったが、その背景にはネット上での存在感の高まりが指摘されている。韓の市長選出馬後、フェィスブックには「韓國瑜ファン後援団」と称するグループが立ち上がり、対抗馬の陳や蔡英文政権や韓に批判的な人物を誹謗中傷するフェイクニュースが頻繁に投稿された。陳陣営は投稿者の中に国外のIPアドレスを特定し、他にも微信（We Chat）を保有する中国当局の検閲や監視に協力する騰訊（テンセント）の社員を名乗る３名の人物も判明している。このことについて、台湾の国立中正大学の林穎佑助教は2015年12月に創設されたサイバー、宇宙、電子など幅広い領域を管轄するPLAの戦略支援部隊

(31) “CHINESE PLA MEMBERS, 54th RESEARCH INSTITUTE” WATED BY THE FBI (2.10.2020)

との関係を指摘している(32)。台湾との関係においては、中国政府の台湾独立に対する反対･阻止の意志として一貫した立場をとっている。2005年制定の「反国家分裂法」は10条の条文で構成されており、注目するべき条文は第６条において、「国は次の各号に掲げる措置を講じて、台湾海峡地域の平和･安定を守り、両岸関係を発展させる」とし、その５号では、「台湾海峡地域の平和・安定の維持および両岸関係の発展に有益なその他の活動を奨励し、推進する」と明記されている(33)。この条文が中国政府の台湾における諜報活動は「内政問題」であり、正当性を主張する根拠としていることが考えられる。その理由の一つとして、中国当局の工作機関が台湾においてこのような政治介入を実行したにもかかわらず、容易に「足跡」がたどられ、周到な隠ぺい工作等が図られていない点である。ロシアと同様に民主主義の価値や信頼を失墜させることも狙いの一つであることが考えられる。他にも中国のSNSの特殊な事情が注目されている。世界中で使用されるLINEやツイッターといったアプリは中国で使用できないことはよく知られる通りであるが、中国版アプリというべき前述の微信（We Chat）は中国企業騰訊（テンセント）が提供し、利用者は中国政府の監視・検閲を受けることになる。インドやネパールのチベット人は70％がこのアプリを利用している。チベット在住の家族と連絡を取る際に必要であり、監視や検閲を承知で利用せざるを得ない事情があるが、ニュースの中に政府に都合のよい多くのフェイクニュースが含まれているとされている(34)。また、2019年の「逃亡犯条例改正案」を契機とする香港の抗議デモにおいては、香港で使用されるツイッターに20万件の不正なアカウントが発見され、ツイッター社は「国家が管理する報道機関」の広告掲載を禁止した。中国では投稿１件ごとに５毛（約

---

(32) ポール・ホワン、「中国サイバー集団が台湾を襲い始めた」『ニューズウイーク日本版』（2019年９月３日号）23-26頁。

(33) 中華人民共和国駐日本国大使館Webサイト、「台湾問題と中国の統一　反分裂国家法（全文）」（2020年５月６日閲覧）

(34) テンジン・ダラ、「微信のチベット侵攻作戦」、「ニューズウイーク日本版」（2019年９月３日号）27-29頁。

７円）が支払われる「五毛党」と呼ばれる工作員が存在し、中国当局の偽情報作戦の一端を担っている(35)。このような中国のデジタル技術を基盤に習近平主席が再構築した権威主義的統治の考え方について、ドイツ・トリーア大学のセバスティアン・ハイルマン教授（Sebastian Heilmann）は「デジタル・レーニン主義（Digital Leninism）」と名づけ、中国政府の都合のよいオンライン情報を流布して情報操作を行い、ビッグデータを用いて国民個人、各企業の行動を監視下に置き統制する制度を作り上げたと分析する。この思想の背景には、マルクスが定義した「物質的な生産力や生産関係の変化が、歴史を動かす原動力となる」という「唯物史観」として、習政権が手に入れたのがデジタル技術の有用性であり、この「デジタル文明」をイデオロギーとして固めつつあるとしている。また、華為技術（Huawei）による5G事業や香港情勢にも触れ、最先端の人工知能（AI）基盤の監視技術の導入に警鐘を鳴らしている。ハイルマン教授の分析を実証している例として、ハイルマン教授自身、2013年、ベルリンに創設された「メルカトル中国研究所（MERICS）」の所長を務めていた際、中国当局からの資金協力者に対する圧力から所長を退いたという過去も明かしている(36)。

近年のこのような諸外国の事例よりも以前から、実際にこのような脅威については論じられていた。2007年、アメリカ海兵隊の研究機関（Center for Emerging Threats and Opportunities）（以下、CETO）の研究員フランク・ホフマン（Frank.G.Hoffman）は、「ハイブリッド脅威（Hybrid threats）」という定義を表し、「ハイブリッド戦争は伝統的な通常戦の終焉を意味するものではないが、21世紀の国防計画に複雑な要因を与えるものである」と予見した上で、「海兵隊の優秀な戦歴、遠征の精神や機転を利かせた研究を活用していく」必要

---

(35)　ジェームズ・パーマー、「デモ隊をディスる中国情報戦の手口」、「ニューズウイーク日本版」（2019年９月３日号）30-31頁。

(36)　読売新聞、「あすへの考　中国サイバー覇権の脅威」（2019年11月24日）６面。

性を強調した(37)。また、ホフマンは1999年に発表されたPLAの喬良（Qiao Liang）と王湘穂（Wang Xiangsui）両大佐による戦略研究の共著『超限戦（Unrestricted Warfare)』について触れ、「大規模な技術の融合は、政治、経済、軍事、文化、外交そして宗教の領域を互いに重複させ、軍事領域や犠牲者の数で戦争の規模を表すことはより時代遅れな考え」になるという両者の考えを紹介している(38)。

このような新しい戦争の概念が注目される中で、「ソフトパワー（Soft power)」とも「ハードパワー（Hard power)」とも異なる、国際社会における新しい影響力として「シャープパワー（Sharp power)」という概念が提示されている。2017年12月、「米シンクタンク全米民主主義基金（National Endowment for Democracy)」は「シャープパワー：権威主義的影響力の高まり」において、「権威主義国家によるシャープパワーの行使は、ハードパワーとは異なり、ステルス性を備え、民主主義の開かれた情報環境を悪用すること」(39)に長けており、「これまでアメリカ、西ヨーロッパ先進国のメディアは、文化、政治の分野でロシアと中国の標的にさらされており、特に孔子学院や大学の協定による、表現の自由や学問の保全性の課題」や、「民主主義制度に脆弱性を抱える国」が権威主義国家の標的にされる傾向があることを警告している(40)。

（4）米国のサイバー戦略

ここまで権威主義的性質を持つとされる国家の事例を取り上げたが、「ハイ

---

(37) Frank. G. hoffman, “CONFLICT IN THE 21ST CENTURY: THE RISE OF HYBRID WARS” Potomac Institute for Policy Studies Arlinton, Virginia (2007) pp.9-10.

(38) Frank.G.hoffman, a.a.o.s.p.22.

(39) “SHARP POWER Rising Authoritarian Influence” INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES NATIONAL ENDOWMENT FOR DEMOCRACY (2017) p.13.

(40) “SHARP POWER Rising Authoritarian Influence” INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES NATIONAL ENDOWMENT FOR DEMOCRACY (2017) p.23.

ブリッド戦争」の特色がみられるアメリカの軍事行動にも注目したい。アメリカはテロ対策としてサイバー空間での諜報活動にリソースを割いてきたことは前述のとおりであるが、2010年には、「スタックスネット（Stuxnet）」と称するマルウェアを使用し、イランの原子力施設を標的にしたサイバー攻撃を行っている。経緯としては2010年11月23日、IAEAが報告書でイランのウラン濃縮活動の一時停止を明らかにし、同年11月29日にはアフマディネジャド大統領がウラン濃縮施設の遠心分離機がコンピュータウイルス感染したことを発表した。これはさかのぼる11月16日にはナタンツのウラン濃縮施設で約8400台の遠心分離機が停止していることをIAEAが確認し、イランは11月22日までに約4600台が再稼働したことをIAEAに報告したものである(41)。このマルウェアはインターネットやUSBメモリを介し、システムの脆弱性を利用してウイルスを拡散し、バックドアを作成することでウイルスの増強や追加を可能とするものである。この攻撃者はWindowsやLinux等のオペレーティングシステムだけでなく、制御システムにも精通しているとも指摘されている(42)。軍事の世界では無線やレーダーの妨害あるいは破壊のために、電波の傍受・解析（ESM）、位置測定を行う電子戦の他に、コンピュータに贋データを送る、データを盗む、贋の命令で誤作動させるなどのサイバー戦（サイバー電子戦）に区別されるが(43)、スタックスネットの事例は後者といえるであろう。

このような情勢のなかでアメリカでは安全保障戦略や国防戦略のさらなる転換を図る動きも出ている。トランプ大統領の下で2017年９月に「国家安全保障戦略（NATIONAL SECURITY STRATEGY）」が発表された。その中でアメリカはこれまでは陸、海、空、宇宙の領域を適切に管理することで国土を保護

---

(41)　小熊信孝、「Sutuxnet―制御システムを狙った初のマルウェア―」、Japan Computer Emergency Response Team Coordination Center（2011）８頁。

(42)　株式会社ラック、「情報セキュリティの現状と動向について」公益財団法人、防衛基盤整備協会（2014）42-43頁。

(43)　井上孝司、「サイバー電子戦のすべて（７）通信妨害から新たな局面へ／多様化する妨害対象　海・空とは異なる『陸上の電子戦』」、「軍事研究」（2020年５月号）、208-214頁。

してきた一方で、サイバー空間は国境を超えることなく、アメリカの政治、経済、安全保障に敵対する能力を国家や非国家に提供しており、インターネットの創始期にはこのような懸念は考慮されていないことから、新たなデジタルインフラの構築の必要性を指摘している(44)。また、悪意ある攻撃者の脅迫、情報戦、虚偽情報により、民主主義制度や世界経済の枠組みが損なわれる可能性や権威主義体制を守るためのツールとして悪用する国の存在を指摘していることからも(45)、近年の「ハイブリッド戦争」を念頭においたものであることがうかがえる。

2018年にジェームズ・マティス国防長官（James Norman Mattis）の署名により発表された「2018年の国防戦略（Summary of the 2018 NATIONAL DEFENCE STRATEGY of The United States of America）」では、安全保障環境の変化に言及し、これまでのアメリカ軍はあらゆる作戦領域において優位性を享受してきたものの、今日では陸、海、空、宇宙、サイバー空間とすべての領域が戦場となっているとして、多次元領域（Multi Domain Operations）の重要性を提示した(46)。また、従来の「対テロ戦争」からの転換を図り、ロシア、中国を「修正主義国家（revisionist powers）」として競争の対象に位置付けている(47)。

2018年から2019年にかけて、日本のメディアでも「米中貿易摩擦」、あるいは「米中貿易戦争」の報道が賑やかであったが、これが単純な通商対立でなかったことは明白であろう。2018年８月までに、下院、上院で可決され、同年８月13日にトランプ大統領によって署名された「米国国防権限法2019（NATIONAL

---

(44) “NATIONAL SECURITY STRATEGY of the United States of America” (12.2017) pp.12–13.

(45) “NATIONAL SECURITY STRATEGY of the United States of America” (12.2017) pp. 31–32.

(46) “Summary of the 2018 NATIONAL DEFENCE STRATEGY of The United States of America” (2018) p.3.

(47) “Summary of the 2018 NATIONAL DEFENCE STRATEGY of The United States of America” (2018) p.2.

DEFENCE AUTHORIZATION ACT FISCAL YEAR 2019）」（以下、NDAA 2019）は、通商関連法の改正を含む政府機関が使用する中国企業情報通信機器の取引禁止や中国、北朝鮮、イラン、ロシアに対する政策の厳格化やインドとのさらなる関係強化などについて広範囲な法制化が行われたものである。まず、このNDAA2019に新たに挿入・規定されたのが「外国投資リスク審査現代化法（FIRRMA）」（以下FIRRMA）と「輸出管理改革法（ECRA）」（以下、ECRA）である。これは「対米外国投資委員会（CFIUS）」（以下、CFIUS）の審査対象となる投資行為が従来の買収、合弁以外にも拡大されている(48)。まず、ECRAの概要については、1758条で「新基本技術の特定及び規制手続・要件」を規定、1753条(a)(2)(f)で「米国法人・米国人の外国軍事諜報サービスへの関与」の新規定、1760条(c)(1)(A)で「違反者の罰則強化」、1757条で「米国政府の米国法人・米国人への輸出管理法令コンプライアンス支援義務」、1761条で「米国政府によるベストプラクティス・ガイドライン策定責務」、1756条(b)で「許可・不許可の審査期間を許可申請後、原則として30日以内とすること」を推奨している(49)。次にFIRRMAの概要であるが、1703条で米国ビジネス関与者がCFIUSの審査対象となる「その他の投資」について、「実質的な非公知情報へのアクセス」が可能になる場合、「役員又は役員に準じる職位」につくことができる場合、また、「米国人の機敏な個人データ」、「重大な技術」、「重大なインフラ」の利用、取得、若しくは開示が挙げられている。「米国ビジネス関与者」については、「米国人の機敏な個人データ」、「重大な技術」、「重大なインフラ」への関与者と定義されている(50)。NDAA2019の889条には、「米国政府機関に対する一定の中国企業の通信・監視関連機器の購入等及びそれら機器を利用している企業等との取

(48)　CISTEC事務局、「米国国防権限法2019の概要」、「CISTECジャーナル」、一般財団法人安全保障貿易情報センター（2018）1頁。“One hundred fifteenth congress of the United States of America AT THE SECOND SESSION” U.S. H.R.5515, (2018)
(49)　CISTEC事務局、前掲論文、3-4頁。
(50)　CISTEC事務局、前掲論文、5-6頁。

引禁止」が規定され、Huawei（華為技術）社、ZTE（中興通訊）社、これらの子会社、関連企業が製造した通信機器やその他中国の複数の企業が提供するビデオ監視機器、通信サービス、ビデオ監視サービスの購入・取得・利用の契約及びその延長・更新が禁止された(51)。この規定が注目される点は、上記のHuawei（華為技術）社、ZTE（中興通訊）社等の指定企業（以下、禁止企業）との取引のある企業も禁止の対象とされることである。要するに、これら禁止企業の部品が一部でも組み込まれた禁止企業以外の他社製品も米国政府機関へ納入することが不可能になる。さらに、禁止企業の部品を使用した製品を販売する企業は、禁止企業の部品を使用していない別の製品も米国政府機関に納入することはできない。このことは、禁止企業と何らかの取引等で関わりのある企業はアメリカ市場から締め出されることを意味し、アメリカ市場の参入を望む企業はサプライチェーンの転換を迫られることになる。もはや経済分野、法律分野までが軍事戦略に組み込まれた一例である。

2018年11月16日、トランプ大統領は「2018年サイバーセキュリティ・インフラストラクチャセキュリティ庁（CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY）」（以下、CISA）CISA法に署名し、CISAが発足した。これは前述の同時多発テロ後に発表された「国土安全保障戦略」発表後の2002年11月25日に設置された、「国土安全保障省（Department of Homeland Security）」（以下、DHS）の傘下にあり、2007年に設立された「国家保護とプログラム総局（National Protection and Programs Directorate）」（NPPD）を再編したものであるが、権限はそのまま残されており、予算は増額されている(52)。CISAはサイバーセキュリティ、インフラストラクチャの保護、緊急事態コミュニケーションを担っている。サイバーセキュリティでは、選挙の保障にも取り

---

(51) CISTEC事務局、前掲論文、７頁。

(52) Cimpanu. Catalin, “Trump signs bill that creates the Cybersecurity and Infrastructure Security Agency”, ZDNet. Retrieved, November 16, 2018, https: //www. zdnet. com / article / trump-signs-bill-that-creates-the-cybersecurity-and-infrastructure-security-agency/（2020年５月14日閲覧）

組んでおり、2016年の大統領選挙を念頭に置いたものと思われる。2020年初めから発生した、COVID-19（以下、新型コロナウイルス）のパンデミックに際しては、米中間で繰り広げられた非難合戦の報道が記憶に新しいが、CISAは５月に「COVID-19虚偽情報活動」という警告を発し、中国政府による誇張された発表やSNS等における新型コロナウイルスに関する虚偽情報について国民への注意喚起を促している(53)。５月13日にはFBIと共同で、保健関係機関、製薬会社、研究機関等に対し、中国政府機関によるネットワーク侵害の標的とされていることを認識し、システム保護のための措置を講じるよう警告した。また、疑わしい活動を行う組織は地元のFBI事務所に通報することも呼びかけ、この警告は英国の「国家サイバーセキュリティ庁（National Cyber Security Agency）」と連携して発していることも明らかにした(54)。このように世界的混乱の中で「ハイブリッド戦争」はより苛烈化していることがわかる。

テロ対策から生まれたアメリカの国家戦略や政府機関は安全保障環境の変化から、テロ組織の監視だけでなく、権威主義国家との競争という新たな展開をむかえている。

３．ドイツの「SNS法」とNATOの危機感

（１）ポピュリスト政党の台頭

2015年、ヨーロッパでは、シリア内戦や、イラクなどでISISの支配地域拡大に伴い、100万人規模の難民がヨーロッパに流入し、その対応をめぐり、EU加盟国の中でも意見は対立した。とりわけドイツのアンゲラ・メルケル首相は、

---

(53) “CISA INSIGHTS COVID-19 Disinformation Activity”, CISA, (5. 2020)

(54) CISA Webサイト、“FBI AND CISA WARN AGAINST CHINESE TARGETING OF COVID-19 RESEARCH ORGANIZATIONS” (5. 13, 2020)
https://www.cisa.gov/news/2020/05/13/fbi-and-cisa-warn-against-chinese-targeting-covid-19-research-organizations（2020年５月14日閲覧）

難民の受け入れに前向きであり、その対応は国内外で議論を呼んだ。第二次世界大戦後のドイツは排外主義を放棄し、トルコやユーゴスラビアなどからの移民の流入を受け入れてきた。産業基盤を支える労働力としての需要も否定できないが、ファシズムやホロコーストに対する反省と人道主義を徹底してきたドイツは西欧諸国の中でも移民や難民の受け入れに対し、比較的寛容な姿勢であったことはよく知られている通りである。一方で、一部ではあるものの非合法のネオ・ナチグループや、いわゆる極右政党なども存在し、1966年からバイエルン州で頭角をあらわし、1969年には連邦議会進出を目指したものの、５％条項に阻まれたドイツ国民民主党（Nationaldemokratische Partei Deutschlands）（以下、NPD）などがあげられる。NPDは2001年に連邦憲法裁判所に違憲申請が行われたが、連邦憲法擁護庁（Bundesamt für Verfassungsschutz）の不正な内偵活動が発覚し、2003年には連邦憲法裁判所が審理を中止する事態となった。この違憲申請はドイツ連邦共和国基本法（Grundgesetz für die Bundesrepublik Deutschland）21条２項に基づくもので、NPDの外国人、ユダヤ人に対する暴力行為が問題視されたものである。この規定は後述する基本法の「戦闘的民主主義（Streitbare Demokratie）」の概念を明文化したものである(55)。近年新しい極右政党としてよく知られるのが2013年創設の「ドイツのための選択肢（Alternative für Deutschland）」（以下、AfD）である。AfDはリーマンショック後の欧州経済危機を発端とする「EU懐疑論」のなかで結党されており、党綱領には「われわれはユーロ通貨圏の整然たる解体を求める、ドイツはユーロを使用しない、ユーロは他国を害する」と表明し、EUの離脱を示唆する文言も含まれている(56)。2016年４月に採択されたAfD党

---

(55)　ドイツ連邦共和国基本法21条２項が根拠規定となっている。「自由で民主的な基本秩序（freiheitliche demokratische Grundordnung）」を侵害し、「ドイツ連邦共和国の存立を危うくすることをめざす政党」は連邦憲法裁判所によって違憲とされ禁止されることとなる。國吉孝志、「ドイツ連邦共和国における政党国家論：「戦闘的民主主義」と政党の違憲問題」、「九州国際大学大学院法政論集」第11号、九州国際大学（2009）93-96頁。

綱領起草者の一人である哲学者ヨンゲン（Marc Jongen）は、2015年夏以降の越境者危機に際し、「国政研究所（Instituts für Staatspolitik）」で行った「移民とティュモスのトレーニング」と名付けられた講演で、メルケル政権の難民受け入れを「巨大な社会的実験」と称し、国家の主権が侵害されただけでなく、国民や国家の「精神政治的（psycho-politisch）」な視点としてこれを「暴力行為」とみなし、「家宅侵入されたかのような感覚で痛みを感じる人々と、むしろ歓迎する人々との分断」を招いたと批判し、プラトン哲学の「気概」を意味する「テュモス（thumos）」という語を用い、2014年以来ドレスデンで起こった西洋のイスラム化に反対する欧州愛国者のデモ「ペギータ」をテュモス発露の証として評価した(57)。

このようなポピュリスト政党の台頭や、社会の分断が起こるなかで、ここでもロシアによるメルケル政権への打撃を狙った世論操作が指摘されている。ベルリンに住む13歳のロシア系ドイツ人の女性が行方不明になり、難民による性被害にあったことを隠ぺいしたとして、ロシア政府がドイツ政府を批判した「リサ事件」では、ロシア系ドイツ人や極右集団によるデモが起こり、後に女性が虚言であったことを認めたものであるが、この情報を広めたのもロシアのメディアやSNSであった。2015年４月にはロシア軍情報機関によるサイバー攻撃により、ドイツの主要サーバー14台が不正アクセスにより、ドイツ連邦議会に属するデータが被害を受けた。この他にもドイツ軍需企業へのサイバー攻撃も相次いでいる。このような動きに対して、ドイツ当局では戦略的コミュニケーション（Strategy Communication）の部隊を創設するなどの対策をとっている(58)。ポピュリズム政党の台頭を利用してロシアが情報戦を仕掛けるケースはドイツのみならず、他の西ヨーロッパ諸国にもみられる。フランス「国民戦

---

(56)　星野智、「ドイツにおける極右ポピュリスト政党の台頭―AfDをめぐって―」、『中央大学社会科学研究所年報』第20号、中央大学（2015）5-6頁。

(57)　三好範英、「越境者の流入と欧州ポピュリズムの台頭」、「国際安全保障」第46巻第４号、国際安全保障学会　（2019）58-59頁。

線（現国民連合）」はロシアによるウクライナ、シリアへの干渉を擁護しており、2014年にロシアは関係する銀行を通じて国民戦線に対し、約1300万ドルを提供したとされている[59]。また、イタリアで2009年に創設された「五つ星運動」は、シリアのアサド政権との国交正常化、ロシアのクリミア併合の承認、イタリアのNATO参加反対、EU脱退などを掲げ、2016年の憲法改正の国民投票では、ロシアのRTが作成した数千人の反対デモの動画が五つ星運動によりSNSに拡散された。その後、2018年３月のイタリア総選挙では、五つ星と同盟（旧北部同盟）が連立政権を樹立している[60]。

（２）ドイツ「SNS法」

越境者危機やポピュリスト政党の台頭により、ドイツではSNSを中心にこのようなフェイクニュースや難民への敵意や憎悪を煽るヘイトスピーチが問題視された。2017年３月14日には、「連邦司法及び消費者保護省の参事官草案（Referentenentwurf）」が公表され、４月５日には連邦政府法案が閣議決定された。同時に連立与党案も提出され、委員会審査の修正の後2017年６月30日、「SNS 法（Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken）」（以下、SNS法）が連邦議会で可決、同年10月に施行され、2018年１月から本格実施に入った[61]。この法律は国内利用登録者200万人以上の「SNS事業者」が対象となり、音楽や職業紹介等の特定の内容に限定されたSNSは対象外となる（１条１項、２項）。「違法なコンテンツ」の定義として、刑法86条（違法な組織のプロパガンダの政策・頒布）、86a条（違法な組織のシンボ

58　ルース・フォーサイス、「ロシアがドイツに仕掛けるハイブリッド戦争」、Web版「ニューズウイーク日本版」（2016年６月２日号）
https://www.newsweekjapan.jp/stories/world/2016/06/post-5234_3.php（５月20日閲覧）

59　一田和樹、『フェイクニュース　新しい戦略的戦争兵器』角川新書（2018）119-120頁。

60　一田和樹、前掲書、124-126頁。

ルの頒布・公然使用）、89a条（国家を脅かす暴力行為の準備）、91条（89a条の罪を文書によりそそのかすこと）、100a条（国家反逆的な事実の歪曲）、111条（犯罪の扇動）、126条（犯罪行為を実行するという脅迫により公共の平穏を乱すこと）、129条から129b条まで（テロ組織の結成等）、130条（民衆扇動罪）、131条（暴力表現）、140条（犯罪行為への報酬の支払い等）、166条（他者の宗教観、世界観の誹謗）、184d条に付随する184b条（ポルノの放送等）、185条から187条まで（名誉毀損的表現）、201a条（盗撮等高度に私的な領域の撮影）、241条（脅迫罪）、269条（法律行為の証拠となるデータの改ざん）の構成要件を満たし、違法性の阻却にあたらないものとされている(62)。その他、「SNS業者」は年間100件の苦情を超える場合、半年に１度報告書をドイツ語で作成した上、１か月以内に連邦官報、自社のWebサイトに公開する義務がある（２条１項）。また、苦情処理手続の策定義務（４条１項１号）が定められ、違法性を審査する自主規制機関を連邦司法庁が認定することになっている。同法の報告義務及び苦情処理手続の策定義務等に反した事業者等は、秩序違反法30条の規定が適用され、最大5000万ユーロ（約64億円）の過料が課せられる(63)。

SNS法の特徴としてはヘイトスピーチ対策に重点が置かれており、前述の刑法187条等の構成要件に該当しない場合、対象外となるためフェイクニュース対策としての効果は限定的である。また、表現規制へとつながることから課題も指摘される。ただ、ドイツでは、基本権として保障される表現の自由についても、前述の「戦闘的民主主義」により濫用を防ぐ規制も存在する。基本法の「戦闘的民主主義」が盛り込まれている規定は、以下のものである。「その目的

---

(61)　神足祐太郎、「ドイツのSNS法」、「調査と情報　―ISSUE BRIEF―」第1019号、国立国会図書館　調査及び立法考査局（2018）３頁。
Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG), Ein Service des Bundesministeriums der Justiz und für Verbraucherschutz sowie des Bundesamts für Justiz - www.gesetze-im-internet.de (2017).

(62)　神足祐太郎、前掲論文、４頁。

(63)　神足祐太郎、前掲論文、4-6頁。

が刑法と抵触する団体あるいは…憲法秩序に反する団体は禁止される。（基本法９条２項）」「出版の自由（５条１項）、教授の自由（５条３項）、集会の自由（９条）、信書、郵便および電話の秘密（10条）、所有権（14条）あるいは庇護権（16条２項）を自由で民主的な基本秩序に反する闘争に濫用するものは、基本権を喪失する。喪失とその程度は連邦憲法裁判所によって決定される。（基本法18条）」、「その目的あるいはその支持者の行動によって自由で民主的な基本秩序を侵害もしくは除去し、あるいはドイツ連邦共和国の存立を危うくすることをめざす政党は違憲である。違憲性の問題については連邦憲法裁判所がこれを決定する。（基本法21条２項）」[(64)]。その意味でSNS法の「違法なコンテンツ」の定義が刑法上の規定の構成要件に限定されていることは、基本法９条２項等との整合性が図られていることがわかる。

（３）欧州要人の意識変化

欧州においてサイバー空間の脅威の高まりが認識されるなかで、そのことを示す例が要人の発言にも表れている。2019年５月23日、ハンブルクで行われた基本法制定70周年を記念するシンポジウムにおいて、ドイツ連邦憲法擁護庁トーマス・ハルデンヴァング長官（Thomas Haldenwang）が「戦闘的民主主義とその敵」と題するテーマの演説を行った。その中で、1933年以来のヴァイマル体制の崩壊からドイツの民主主義の復活にふれ、基本法起草者の一人であるカルロ・シュミット（Carlo Schmid）の言葉を引用し、「必要であれば、民主主義を悪用し人々を攻撃する者に対しては不寛容になる勇気が求められる」として基本法制定の理念を述べたうえで、1977年の「ドイツの秋」における当時ヘルムート・シュミット首相（Helmut Heinrich Waldemar Schmidt）のドイツ赤軍（RAF）によるテロとの戦いを称え、近年のISISのようなITを活用した現代

(64) 國吉孝志、前掲論文、49頁。

のテロの特徴から、サイバー空間における過激主義の脅威について言及し、今日ではSNSが過激派に新たな舞台を提供していることを指摘した。制定から70年たった今こそ「自由で民主的な基本秩序」を祝福する理由を見つめなおすときであると述べた(65)。同日、NATOのイェンス・ストルテンベルグ事務総長（Jens Stoltenberg）はロンドンの「国際サイバーセキュリティセンター」で行われた「サイバー防衛誓約会議」において、サイバー攻撃について、「１度の攻撃が数十億ドルの損害を与え、グローバル企業を停滞させ、民主主義を弱体化させ、軍事力に重大な影響を与える」可能性を指摘し、「NATOの代表者はサイバー攻撃にNATO条約第５条が適用されることに同意」したことで、同盟国に対する攻撃が集団的自衛権の発動要件となる新たな軍事領域に指定した。また、この会議ではサイバー防御に関する教育とトレーニングに重点を置くことを定め、NATOを超えた連携、とりわけEUとの協力の強化を提唱している(66)。このことは、後述する、連合体やその取り組み、また、NATOで研究された「タ

---

(65)　ドイツ連邦憲法擁護庁Webサイト“Die wehrhafte Demokratie und ihre Feinde” Rede von BfV-Präsident Thomas Haldenwang auf dem Symposium „70 Jahre Verfassung − 70 Jahre Schutz“ des LfV Hamburg am 23. Mai 2019
https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/vortraege/rede-p-haldenwang-20190523-symposium-lfv-hamburg（2020年５月22日閲覧）

(66)　北大西洋条約機構 Webサイト“Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London” 23. May 2019
https://www.nato.int/cps/en/natohq/opinions_166039.htm（2020年5月25日閲覧）
NATO条約第５条では、「締約国は、ヨーロッパまたは北米における同盟国の１つ以上に対する武力攻撃は、同盟国すべてに対する攻撃と見なすことに同意する。そのような武力攻撃が発生した場合、国連憲章第51条により認められた個別的又は集団的自衛権を行使し、北大西洋地域の安全を回復、維持するため、武力の使用を含む必要と認める行動など、他の締約国と個別または共同で、攻撃された締約国を支援する。」と規定されている。原文は以下の通りである。
The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

リンマニュアル2.0」にもみることができる。

（４）米国との連携の動き

前述の2016年のアメリカ大統領選挙におけるロシアの介入、干渉はアメリカとヨーロッパ諸国を連携させる動きも見せている。アメリカのドイツマーシャル基金によって設立された「民主主義を守る同盟（Alliance for Securing Democracy）」（以下、ASD）は権威主義国家による民主主義の弱体化、妨害を抑止、防御する上での包括的な戦略を策定し、虚偽情報、悪質金融、新技術、選挙の保全、経済的束縛、サイバーセキュリティ等の各州専門家で構成されている(67)。特に虚偽情報に対する対策として、「ハミルトン68（Hamilton68）」（バージョン2.0）と称するダッシュボードにより、ツイッター、ユーチューブ等のメディアに含まれるロシア及び中国のメッセージについて分析する視点を提供するものであるが、ロシア、中国に起因する情報の可能性の表示にとどめ、発信元や関係者に両国のプロパンガンダと結びつけることには慎重な姿勢を示している(68)。ASDはアメリカを含む複数のヨーロッパ諸国が参加する同盟であるが、新たな脅威が広がる中で今後の更なる進展が予想される。

また、前述の新型コロナウイルスパンデミックをめぐる情報戦に際して、EUの外交を担う機関「欧州対外行動局（European External Action Service）」（以下、EEAS）は「EU vs DISINFO」という特設サイトの中で、新型コロナウイルスパンデミックをめぐる虚偽情報の評価をまとめた報告書を５月20日に更新している。それによると、クレムリン発（ロシア）の英語の宣伝メディアが４月後半には三つ以上みられ、オランダの「総合情報・安全保障局」はオランダ語

---

(67) 民主主義を守る同盟Webサイト“Mission Statement”
https://securingdemocracy.gmfus.org/about-us/（2020年５月25日閲覧）

(68) 民主主義を守る同盟Webサイト“Hamilton 2.0 Dashboard”
https://securingdemocracy.gmfus.org/hamilton-dashboard/（2020年５月25日閲覧）

が使われる多くのSNSの中で「EUの連帯欠如」などのロシアの主張する物語が共有されていることを報告した。中国についても「他国の時間を稼ぐために犠牲を払った」という主張や、（中国の対応こそが）「他国が従うべきモデル」であるという主張がなされており、米国政府とその対応を嘲笑する方向にシフトしていることが指摘されている。その他にも「アメリカが発生源」と主張した中国外務省代表のツイートをロシアRTが引用する形で記事を発表するなどの動きも見られた。またISISのようなテロ組織もパンデミックの混乱と隙をついた攻撃を呼びかけるなどの動きがみられ、他にもバルト三国におけるNATOの存在感の弱体化をねらい、西側諸国のパートナー間に不信を植え付け、報道機関の言論を脅かそうという試みにこのパンデミックが活用されていることも警告している(69)。

ヨーロッパ諸国ではリーマンショック後の金融危機以来、越境者危機、ポピュリスト政党の台頭、英国のEU離脱等、数多くの混乱がみられた。その中でサイバー空間における情報戦は激しさを増し、より巧妙に洗練されている。一方で、NATOを中心にその脅威は共有され、対策も模索されつつある。このNATOの危機感こそが、サイバー攻撃への軍事的対抗手段として国際法における位置づけの研究を推進し、完成させたのが「タリンマニュアル2.0」である。

4．「タリンマニュアル2.0」

ロシア戦勝記念日の2006年５月９日、エストニアの首都タリンのソビエト軍

---

(69) 欧州対外行動局Webサイト“EEAS SPECIAL REPORT UPDATE: SHORT ASSESSMENT OF NARRATIVES AND DISINFORMATION AROUND THE COVID-19 PANDEMIC (UPDATE 23 APRIL — 18 MAY)” COVID-19 DISINFORMATION EEAS SPECIAL REPORT 20. May 2020
https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid19-pandemic-updated-23-april-18-may/（2020年５月25日閲覧）

人像付近でロシア系住民による非ロシア系住民への暴行事件が発生した。これを受けた2007年３月のエストニア政府によるソビエト軍人銅像の郊外の戦没者墓地移設決定をめぐり、ロシア系住民の抗議活動は暴動に発展し、死者１名、負傷者約数百名、逮捕者約1300名を出す騒動となった。モスクワのエストニア大使館前では反対デモに加え、在ロシアエストニア大使の襲撃も発生し、この一連の事件はエストニア、ロシア両国の民族主義的対立が露呈する結果となった。このような状況のなかで2007年４月27日、エストニアの政府機関および民間のウェブサイトが単純なDos（Denial of Service）攻撃と呼ばれるサイバー攻撃の被害を受けはじめ、その後エストニアのインターネットサービス・プロバイダーのDNS（Domain Name System）が、複数のボットネットからのDDos（Distributed Denial of Service）攻撃に拡大し、５月９日から10日には政府機関のものを含む58のウェブサイトが中断した(70)。

このような計画的、組織的なサイバー攻撃により、国家機能が不全に陥る危機を体験したエストニアでは2008年、NATOサイバー防衛センター（Cooperative Cyber Defence Center of Excellence, CCD COE）がタリンに設立された。そこでサイバー攻撃に対する、国際法の適用を条文として整理し、解説を加えたのが「タリンマニュアル2.0」である。本書は、2013年に刊行された「サイバー戦に適用される国際法に関するタリン・マニュアル」（Tallinn Manual on the International Low Applicable to Cyber Warfare）が大幅な加筆により刷新されたものとなっている(71)。「第一部」から「第四部」で構成され、20の項目に分けられ、規則１から規則151の条文が規定されている。項目で見ていくと、１「主権」、２「相当の注意」、３「管轄権」、４「国家責任法」、５「それ自体は国際法によって規律されないサイバー行動」、６「国際人権法」、７

⑺⓪　山口嘉大、「サイバー防衛における官民連携の強化について　―エストニア共和国との比較を通じて―」、「防衛研究所紀要」第21巻第１号、防衛研究所（2018）161-163頁。

⑺①　中谷和弘、河野桂子、黒崎将広、『サイバー攻撃の国際法　―タリンマニュアル2.0の解説―』信山社（2018）３頁。

「外交及び領事法」、8「海洋法」、9「航空法」、10「宇宙法」、11「国際電気通信法」、12「平和的解決」、13「干渉の禁止」、14「武力の行使」、15「集団的安全保障」、16「武力紛争法一般」、17「敵対行為の遂行」、18「特定の人、物及び活動」、19「占領」、20「中立」となっている(72)。本書の編著者であるミヒャエル・N・シュミット教授（MICHAEL N. SCHMITT）はアメリカ海軍大学校のストックトン国際法研究所の会長、イギリスエクセター大学では、国際公法学の教授を務め、NATOサイバー防衛センターの上級研究員も兼務する国際法のエキスパートである(73)。サイバー攻撃といってもその活動や行為、目的は幅広く、「タリンマニュアル2.0」の中で14「武力の行使」にある第２節自衛の規則71「武力攻撃に対する自衛」では、「武力攻撃の水準に至るサイバー行動の目標となる国家は、固有の自衛権を行使することができる。サイバー行動が武力攻撃に該当するか否は、その規模及び効果による。」と明記される。規則69で定義される武力の行使の水準に至るサイバー行動の定義について、国連憲章２条４項は基準を示していないものの、ニカラグア事件におけるICJの採用した「規模及び効果（scale and effects）」に注目し、「ある政府への信頼を揺るがすことだけを企図した非破壊的なサイバー行動や、経済への負の影響を引き起こすことを企図した電子商取引の禁止だけ」では武力の行使にならず、一方で、他国との敵対行為に従事する組織にサイバー攻撃に用いるマルウェアや訓練を提供することは「武力の行使」が成立するとしている。しかし、規則71の「武力攻撃」は「武力行使」とは異なり、「大多数の人間を殺傷するか、又は財産に重大な損害若しくは破壊をもたらす」水準の規模及び効果を持つサイバー行動であると定義している。その意味では、前述の2010年のアメリカによる「スタックスネッ

---

(72)　中谷和弘、河野桂子、黒崎将広、前掲書、7-12頁。

(73)　MICHAEL N. SCHMITT, LIIS VIHUL, “TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS”, NATO Cooperative Cyber Defence Centre of Excellence (2017) p.1「タリンマニュアル2.0」の原書については本書を参照。

ト」を用いたイラン原子力施設へのサイバー攻撃は「武力行使」、「武力攻撃」の水準を満たすものであると考えられるが、「武力攻撃」であるか否かの見解については専門家の意見は一致していない(74)。

一方でサイバー行動には、「武力行使」や「武力攻撃」の水準を満たさない「グレーゾーン」ともいうべき事態も当然ながら想定され、そのような状況を踏まえた規則についても注目するべき点である。

11「国際電気通信法」の規則62「サイバー通信の停止」の(a)では「国家は、部分的に又は完全に、自国領域内における国際サイバー通信業務を停止することができる。当該停止の即時の通知が他国に対してなされなければならない。」とし、(b)では「国家は国内法令、公の秩序若しくは善良の風俗に反すると認められ、又は国家の安全にとって危険である私用のサイバー通信の伝達を停止することができる。」と国際電気通信連合（ITU）憲章35条及び34条２項に基づき明記されている。本規則の例として、2011年「アラブの春」に際し、エジプト政府が行ったインターネット及び携帯電話への接続遮断があげられるが、「すべての公の目的のための外交使節団又は領事機関の自由なサイバー通信」を認める規則42との関連と、規則62(b)の「私的な」ものでない外交使節団や領事機関の公的なサイバー通信は停止できない(75)。また、13「干渉の禁止」の規則66条「国家による干渉」では「国家は、他国の国内又は対外事項に、サイバー手段による場合を含め、干渉してはならない」としているが、干渉（intervention）は強制的要素を持たない介入（interference）と区別した上で、ある国家が特定の国家に対象に、プロパガンダをインターネットで展開することや、サイバー諜報についても相手の選択の自由が奪われず、強制的要素をもたないため、強制的な干渉とならないというのが専門家の見解である。一方、前述のDDosオペレーション等により特定の国家の選択の自由を奪う、またその国の意志に反

(74) 中谷和弘、河野桂子、黒崎将広、前掲書、75-78頁。
(75) 中谷和弘、河野桂子、黒崎将広、前掲書、63-64頁。

する結果を引きだすための積極的な行為は干渉にあたるとされている(76)。規則66条からも、ロシアによるエストニアへのサイバー攻撃はこの干渉にあたると考えられる。

前述のNATOのストルテンベルグ事務総長が言及したサイバー攻撃におけるNATO条約第５条の適用に関連して、規則74「集団的自衛」では「自衛権は集団的に行使することができる。武力攻撃となるサイバー行動に対する集団的自衛権は、被害国の要請に基づきかつ当該要請の範囲内においてのみ行使することができる。」として、国連憲章第51条及び慣習国際法上、国家は、集団的自衛権により、サイバー武力攻撃を受けたすべての国と共同防衛を行うことを認め、必要性、均衡性、急迫性及び即時性の要件を設けている(77)。規則74に明記される通り、「集団的自衛」の対象となるのは前述の規則71で挙げた「武力攻撃」である。

「タリンマニュアル2.0」の概観について、これまで述べてきた「ハイブリッド戦争」の観点を中心に述べたが、本マニュアルは現在も発展途上であり、今後の国際的枠組みや、更なる脅威に対応しながら今後の更新が期待されるものである。

５．我が国の法整備の現状

（１）サイバーセキュリティ基本法

我が国においてもサイバーセキュリティ強化をめぐり、これまで継続して議論されてきた。IT技術の進展により、我が国の企業の経済活動や官公庁の機密情報の保護が喫緊の課題となっている。とりわけ、防衛省及び防衛関連企業の

(76)　中谷和弘、河野桂子、黒崎将広、前掲書、71-72頁。
(77)　中谷和弘、河野桂子、黒崎将広、前掲書、82頁。

防衛秘密にあたる情報はこれまでもサイバー攻撃の標的にさらされ、我が国のみならず、同盟国にとっても深刻な脅威となっている。本項では、サイバーセキュリティを中心に、通商政策の視点からも「ハイブリッド戦争」を視野に入れ考察したい。

我が国のサイバーセキュリティの基本方針を規定した法律として、「サイバーセキュリティ基本法」が挙げられる。2014年11月に成立した本法は、サイバーセキュリティの概念に加え、基本理念に基づく施策、国、地方公共団体の責務を明確化したものである。本法２条では、サイバーセキュリティについて、「情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性および信頼性の確保のために必要な措置」が講じられ、「その状態が適切に維持管理されていること」と定義した上で、４条から７条では、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者、教育研究機関の努力義務を定めている。また、12条に基づき政府はサイバーセキュリティ戦略を策定、24条では、基本施策の総合的かつ効果的な推進のため、内閣へのサイバーセキュリティ戦略本部の設置が明記されている[78]。これに基づき2015年１月９日、内閣に「サイバーセキュリティ戦略本部（NISC）」（以下、NISC）が設置された。NISCは、内閣官房副長官補をセンター長とし、副センター長２名を含む内閣審議官３名、非常勤のサイバーセキュリティ参与１名の４名の指揮の下、「基本戦略（総括・第１・第２）」、「国際戦略」、「政府機関総合対策」、「情報統括」、「事案対処分析」、「東京2020」、「重要インフラ（第１・第２）」のセクションに区分されている[79]。サイバーセキュリティ基本法の基本理念としては３条１項において、「情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要である」とした上で、６条では、「重要社会

---

[78] 大沢秀介、新井誠、横大道聡　編著、前掲書、（2017）390-391頁。

[79] 内閣サイバーセキュリティセンターWebサイト、「サイバーセキュリティセンター（NISC）とは」https://www.nisc.go.jp/about/index.html（2020年６月10日閲覧）

基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする」と国の責務を明確化し、14条では「国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする」と規定するものの、民間の調査機関が提言する攻撃者へのより踏み込んだ情報収集のための法整備には至っていないのが現状である(80)。

サイバーセキュリティ基本法の守秘義務にともなう罰則規定については、第５章の38条で規定されている。17条で「サイバーセキュリティに関する施策の推進に関し必要な協議を行うため」の「サイバーセキュリティ協議会」を組織するとした上で、17条４項には「協議会の事務に従事する者又は従事していた者」が、「正当な理由がなく、当該事務に関して知り得た秘密を漏らし、又は盗用してはならない」としている。また、31条１項の１号と２号で規定される「当該事務の一部」を委託された法人については、31条２項で、「事務の委託を受けた法人の役員若しくは職員又はこれらの職にあった者は、正当な理由がなく、当該委託に係る事務に関して知り得た秘密を漏らし、又は盗用してはならない」とし、これらの規定に違反した者は「一年以下の懲役又は五十万円以下の罰金に処する」と規定している。

（２）我が国の安全保障政策の転換

サイバーセキュリティ基本法の附則２条では、「政府は、武力攻撃事態等及び存立危機事態における我が国の平和と独立並びに国及び国民の安全の確保に関

(80)　大沢秀介、新井誠、横大道聡　編著、前掲書、（2017）391-392頁。

する法律（平成十五年法律第七十九号）第二十一条第一項に規定する緊急事態に相当するサイバーセキュリティに関する事象その他の情報通信ネットワーク又は電磁的記録媒体を通じた電子計算機に対する不正な活動から、国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるもの等を防御する能力の一層の強化を図るための施策について、幅広い観点から検討するものとする」と明記されており、この規定が後の「平成31年度以降に係る防衛計画の大綱について（30大綱）」（以下、30大綱）とともに策定された「中期防衛力整備計画（2019）」（以下、中期防2019）への布石であったとみることも可能であろう。そこで、30大綱および中期防2019の概観についても述べていきたい。

平成30年12月18日に閣議決定された30大綱では、「策定の趣旨」の中で、「宇宙・サイバー・電磁波といった新たな領域については、我が国としての優位性を獲得することが死活的に重要となっており、陸・海・空という従来の区分に依拠した発想から完全に脱却し、全ての領域を横断的に連携させた新たな防衛力の構築に向け、従来とは抜本的に異なる速度で変革を図っていく必要がある」[(81)]とし、従来の「統合機動防衛力」に加え新たな刷新が図られている。Ⅱの「我が国を取り巻く安全保障環境」については、1「現在の安全保障環境の特徴」として「自らに有利な国際秩序・地域秩序の形成や影響力の拡大を目指した、政治・経済・軍事にわたる国家間の競争が顕在化している」ことや、「軍や法執行機関を用いて他国の主権を脅かすことや、ソーシャル・ネットワーク等を用いて他国の世論を操作することなど、多様な手段により、平素から恒常的に行われ」ており、このような「グレーゾーン」が継続的に増加・拡大した結果、重大な事態へ発展する危険性を帯びていることを指摘したうえで、「いわゆる『ハイブリッド戦』のような、軍事と非軍事の境界を意図的に曖昧にした現状変更の手法は、相手方に軍事面にとどまらない複雑な対応を強いてい

(81) 「平成31年度以降に係る防衛計画の大綱について」（平成30年12月18日閣議決定）1-2頁。

る」[82]と明記された。この他にも各所において「宇宙・サイバー・電磁波」領域における対策の必要性が言及され、（２）の「我が国の防衛力の強化」のイ「真に実効的な防衛力―多次元統合防衛力」では、「今後の防衛力については、個別の領域における能力の質及び量を強化しつつ、全ての領域における能力を有機的に融合し、その相乗効果により全体としての能力を増幅させる領域横断（クロス・ドメイン）作戦により、個別の領域における能力が劣勢である場合にもこれを克服し、我が国の防衛を全うできるものとすることが必要である」[83]と、前述の米国国防戦略において定義された、「多次元領域（Multi Domain Operations）」に対し、我が国では、「領域横断（Cross Domain）」と定義している。

30大綱と同じく、平成30年12月18日に閣議決定された中期防2019は、Ⅰ「計画の方針」として、「統合機動防衛力の方向性を深化させつつ、宇宙・サイバー・電磁波を含む全ての領域における能力を有機的に融合し、平時から有事までのあらゆる段階における柔軟かつ戦略的な活動の常時継続的な実施を可能とする、真に実効的な防衛力として、多次元統合防衛力の構築に向け、防衛力の大幅な強化を行う」とし、１「領域横断作戦を実現するため、優先的な資源配分や我が国の優れた科学技術の活用により、宇宙・サイバー・電磁波といった新たな領域における能力を獲得・強化するとともに、新たな領域を含む全ての領域における能力を効果的に連接する指揮統制・情報通信能力の強化・防護を図る」[84]と明記したうえで、指揮系統、部隊運用、装備品等のあらゆる項目において、「領域横断作戦」への対応を求めている。一方、30大綱および中期防2019で大きく注目されたのは、ヘリコプター搭載型護衛艦（DDH）への短距離離陸・垂直着陸（STOVL）戦闘機の搭載やスタンド・オフ・ミサイル等の装備であり、

---

82 「平成31年度以降に係る防衛計画の大綱について」（平成30年12月18日閣議決定）2-3頁。
83 「平成31年度以降に係る防衛計画の大綱について」（平成30年12月18日閣議決定）９頁。
84 「中期防衛力整備計画（平成31年度～平成35年度）について」（平成30年12月18日閣議決定）1-2頁。

各種メディアにも大きく取り上げられたが、これらの装備品の能力は指揮、統制、通信、コンピュータ、情報、監視、偵察（C4ISR）に特化したものとして、戦闘システム全体の一部に組込まれたものであり、個別の視点から評価するべきではない。我が国の安全保障政策が「領域横断作戦」や「ハイブリッド戦争」を重視せざるを得ない急激な安全保障環境の変化により、これを無視できない段階に達しているのである。

アメリカやヨーロッパ諸国同様に、我が国においてもサイバー攻撃の被害は継続して発生している。攻撃国、攻撃目標についても多様かつ広範囲で、とりわけ国民の生命や財産に係り、同盟の結束を揺るがしかねない防衛秘密情報への不正アクセスは深刻な問題である。最近の事例では、2019年６月に、三菱電機を含む複数の防衛産業が係る防衛装備庁から提供された最新の「高速滑空ミサイル」の「性能要求事項」が三菱電機から流出していた疑いが発覚し、防衛省が調査に乗り出した。この情報は特定機密保護法の指定する「特定秘密」の対象とはならないものの、性能要求として射程や耐熱性、推進力等の基本性能が記されていた。犯行の疑いがもたれているのは、「ブラックテック」と「ティック」と呼ばれる中国系ハッカー集団で、前者は、武漢、後者は上海に拠点を置くPLAの部隊と連携し、軍の監督指揮下にあるといわれている(85)。このような中、サイバー空間においても日米の連携は深まっている。2019年４月、ワシントンで開催された日米外務・防衛担当閣僚会合（２プラス２）では、「日米はサイバー攻撃が、一定の状況で、日米安保条約第５条が適用される『武力攻撃』とみなしうると確認した」ことを、ポンペオ国務長官は明言している。一方で、河野太郎防衛大臣によると、日本政府は「サイバー空間でも専守防衛が前提で、関係する国内法、国際法を順守する考えに変わりはない」という立場をとっており、刑法の「ウイルス作成罪」や憲法21条の「通信の秘密の保護」の侵害のおそれからも、米軍の軍事戦略とは異なる自衛隊のサイバー空間での共同対処

(85) 朝日新聞、「最新ミサイル性能漏洩か」（2020年５月20日）１面。

に多くの課題が残されているのも事実である(86)。このような課題について検討するうえで、前述の「タリンマニュアル2.0」における国際法の研究は、今後の我が国のサイバーセキュリティや安全保障政策に与える影響は決して小さくないといえる。「平時」と「有事」の区別が非常に困難な安全保障環境のなかで、防衛省による対処だけではなく、関係省庁が連携しセクショナリズムを排したうえで、平時からの警戒、対処が求められている。

（3）通商・金融分野へ拡大する安全保障政策

2020年４月１日、日本政府は、「国家安全保障会議」に「経済班」を発足させ、安全保障上の課題として経済分野における政策の立案や関係省庁の調整を担当し、国内の大学や研究機関における軍事転用可能な先端技術の保護・育成、外国企業による買収、投資の審査、次世代通信規格5Gをめぐる主導権争いへの対応等の対策に取り組む姿勢を示しており、米中対立が激化する中、経済分野での安全保障政策の連携も強まっている(87)。

2020年４月30日には、「対内直接投資等に関する政令等の一部を改正する政令」が公布され、同年６月７日には「改正外為法及び関連改正政省令・告示の

---

(86) 朝日新聞、「サイバー戦想定　日米演習」（2020年５月20日）２面。
「ウイルス作成罪」については、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」法律第七十四号（平二三・六・二四）により、刑法の一部を改正したものである。「不正指令電磁的記録作成等」について、刑法168条２項において、「正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する」とし、１項では、「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」、２項では、「前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録」と定義している。
衆議院Webサイト、「第177回国会　制定法律の一覧」
http://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/17720110624074.htm（2020年７月２日閲覧）

(87) Web版読売新聞、「『5G』主導権争いに対応…国家安保局に『経済班』」（2020年４月１日）
https://www.yomiuri.co.jp/economy/20200401-OYT1T50123/（2020年７月２日閲覧）

施行及び全面適用」となった(88)。この改正で特に注目される点は、「国の安全等を損なうおそれのある投資への適切な対応」として、「事前届出の対象の見直し」がおこなわれた。「指定届出業種（155業種）」とされていた対象は、改正により、「指定業種のうちコア業種の分野」と「指定業種のうちコア業種の分野以外のもの」に分類され、「指定業種のうちコア業種の分野」の詳細については、「武器」、「航空機」、「宇宙関連」、「原子力関連」、「軍事転用可能な汎用品」、「サイバーセキュリティ関連」、「電力業」、「ガス業」、「通信業」、「上水道業」、「鉄道業」、「石油業」の12業種と分類された(89)。新型コロナウイルスの感染拡大をうけ財務省は、ワクチンや医薬品、人工呼吸器等の高度医療機器も「コア業種」に追加する動きをみせており、今後もリストが更新されていくことが予測される(90)。

このように我が国においても「ハイブリッド戦争」をめぐる政策や法整備は通信や経済を含む広範囲な分野が安全保障政策に組込まれつつあり、防衛省及び自衛隊の専門性を超えた課題を抱えている。その対応は関係省庁のみならず、企業、教育機関、市民社会が連携してさまざまな脅威に対応することが求められる。国民一人ひとりが無意識のうちに諜報活動や情報戦、心理戦に徴用されてしまう危険性を内包しているのが、かつての冷戦や対テロ戦争にもない現代の戦争の特徴である。市民社会がこのような脅威に対応していくためには学校教育においても、従来の防犯・防災教育に加え、情報通信教育のなかで広い視野に立った啓発活動を展開することで、我が国の平和主義や健全な民主主

---

(88) 財務省Webサイト、「『対内直接投資等に関する政令等の一部を改正する政令』について」、（2020年４月24日）
https://www.mof.go.jp/international_policy/gaitame_kawase/press_release/20200424.htm（2020年７月２日閲覧）

(89) 財務省、「『対内直接投資等に関する政令等の一部を改正する政令』について」（2020年４月24日）

(90) Web版日本経済新聞、「外為法リスト、対象拡大　重点審査558社に　日産など追加」（2020年６月５日）
https://www.nikkei.com/article/DGXMZO60044800V00C20A6EA4000/（2020年７月２日閲覧）

義の擁護につながり、基本的人権の保障をより確実なものへと発展させることが期待される。

おわりに

1991年のイラクによるクウェート侵攻を発端に勃発した湾岸戦争（Operation Desert Storm）は、トマホークミサイルやステルス戦闘機、レーザー誘導爆弾等の各種ハイテク兵器が多用され、「ニンテンドーウォー（Nintendo War）」とも称されるほど、従来の戦争の常識を覆した。西側諸国を中心とした多国籍軍の革新的な軍事力を目の当たりにしたロシアや中国は、軍事力の近代化の必要性を痛感したといわれている。同時に湾岸戦争の「ピンポイント爆撃」の映像はメディアに公開され、イラクの残虐性を証言したクウェートの少女が国際社会に与えた影響力など、単純なハイテク戦争にとどまらず、情報戦としての側面も持ち合わせていたといえるであろう。このような西側優勢の環境下での軍事作戦はコソボ紛争におけるNATO軍事介入（Operation Allied Force）でも継続して行われた。2000年代に入ると、「対テロ戦争」の陰で、NATOの東方拡大に焦りと不満を抱えたロシアは、2008年８月、ジョージアに進攻し、南オセチア戦争（Russian-Georgian War）を引き起こした。当時世界が北京オリンオリンピックに注目する最中に敢行された電撃作戦は、情報戦を含むものでもあり、まさに「ハイブリッド戦争」の試作段階として、ウクライナをめぐる前哨戦であったとも考えられる。中国については、1989年６月の天安門事件以降、西側諸国の批判や制裁を受け、外交的孤立の中で、近代化や改革開放政策の鈍化にもつながった。後の経済改革で進められた社会主義市場経済は、海外投資を呼び込み、2000年代には「世界の工場」としての地位確立に加え、2010年代にはGDP世界第２位の経済大国へと中国を押し上げた。このような中国の国家戦略は決して経済成長のみを見通したものではなく、国際社会における政治的影響力拡大や領土的野心が根底にあったことは、現在の中国の動向からも否定で

きるものではない。2020年の新型コロナウイルスの感染拡大の中で中国当局が展開した、「マスク外交」や医療スタッフ派遣等の戦略的コミュニケーション（Strategy Communication）は思惑に反し、欧米諸国の不信感や反感を招いた。西太平洋地域に展開する米海軍空母打撃群（Carrier Strike Group）が一時機能不全となった中で、南シナ海や東シナ海での活動を活発化させたPLA海軍の動きは、我が国の安全保障にとっても決して無視できるものではない。香港では前述の2019年「逃亡犯条例改正案」に続き、2020年には、「国家安全法」が６月30日に中国全人代常務委員会で可決され、中国に対する国際社会の評価は今後より厳しいものへと変わっていくであろう。アメリカ大統領選挙を目前に控えた2020年８月現在、米中関係は悪化の一途をたどり、冷戦ともいえる様相を呈している。このような権威主義国家による「ハイブリッド戦争」に用いられるツールであるインターネットはAPANETを前身とし、かつては核攻撃から通信統制を守るための米軍のニーズで研究され、米国政府の独壇場であった。1990年代から商用化されたインターネットは現在となってはスマートフォンやタブレットにも接続され、情報戦兵器としての可能性を秘めるに至った。戦争とは異なるものの、2020年の米国に広がったブラック・ライブズ・マター運動（Black Lives Matter）はミネソタ州ミネアポリスで発生した警察官のアフリカ系市民への危険かつ不適切な拘束により、死に至らしめる結果となった状況を市民にスマートフォンで撮影され、SNSで拡散されたことで明らかになった。ヨハネス・グーテンベルクの活版印刷機が、1517年のマルティン・ルターの活動の結果である宗教改革に影響を与え、後の長い戦争につながったことからも、メディアと戦争との関係は不可分なものであるといえる。これまで多くの軍需発明品が民生品にスピン・オフされることが常とされてきたが、近年では民生品が軍需品へスピン・オンされていくことも珍しくない。そのため、現在の安全保障は軍事機密や防衛秘密にかかわらず、あらゆるハイテク製品が戦略物資となりうる。その意味で、「ハイブリッド戦争」は軍事と非軍事、有事と平時の線引きが曖昧になっているところに問題の本質がある。そのため、米国の「国

防権限法2019」や我が国の「改正外為法」のように、通商や金融の分野からも安全保障政策を考える必要性が生じている。また、「ハイブリッド戦争」の最も深刻な問題は、自由主義・民主主義国家の抱えるジレンマである。言論統制が可能な権威主義国家とは異なり、表現や思想の自由が保障された自由主義・民主主義国家は「ハイブリッド戦争」への対抗策は脆弱にならざるを得ない。それでも自由主義・民主主義国家は自由や人権を保障し、健全な民主主義を発展させ情報リテラシーを高めていくことが重要である。そのためには政府やインテリジェンス・コミュニティ（Intelligence community）は連携を強化し、オシント（Open-source intelligence）を適切に遂行するなかで、国民が憲法保障や安全保障、インテリジェンスに対して正しく理解を深めることこそがこの脅威に対する対抗策であると考えられる。最後に、2020年６月下旬の河野太郎防衛大臣によるイージスアショア配備断念の判断を受け、ミサイル防衛の代替案として敵基地攻撃能力（相手領域内でも弾道ミサイル等を阻止する能力）についての議論が自民党国防部会および安全保障調査会で議論され、７月31日にはその提言案が了承された。前述のとおり、政府はサイバー攻撃においても専守防衛の方針を固守しており、整合性を欠いているといわざるを得ない。弾道ミサイル等による攻撃に匹敵するサイバー攻撃も当然想定されることから、敵基地攻撃能力については、ミサイル防衛に限定されず、サイバー攻撃を含めた「ハイブリッド戦争」に対応した領域横断的な政策判断が求められ、今後の課題として注視されるところである。