一章一節

（1） *Lowy Institute Asia Power Index 2023 Edition.* https://power.lowyinstitute.org/data/military-capability/.

（2） 二〇二一年のウクライナの防衛予算は四二・七億ドル、ロシアの防衛予算は四五八億ドルであった。IISS. *The Military Balance 2022*. Routledge, 2022.

（3） 二〇二一年のウクライナのGDPは一八一〇億ドル、ロシアのGDPは一兆六五〇〇億ドルであった。IISS, Ibid.

（4） いずれも数字は、IISS, Ibid. より著者集計。

（5） Zabrodskyi, Mykhaylo, et al. “Preliminary Lessons in Conventional Warfighting from Russia’s Invasion of Ukraine: February–July 2022.” *RUSI Special Report*, Royal United Services Institute, 30 November 2022, https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

（6） Zabrodskyi, et al., Ibid.

（7） ウクライナにおける陸上戦闘の推移については、Institute for the Study of War. *UKRAINE CONFLICT UPDATES.* https://www.understandingwar.org/backgrounder/ukraine-conflict-updates.を参照。

（8） 海上における戦闘については、Pedrozo, Raul.“Russia-Ukraine Conflict: The War at Sea.” *International Law Studies*, vol. 100, 2023, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3038&context=ils.を参照。

（9） フェドロフ副首相兼デジタル化担当大臣 X（旧ツイッター）投稿 https://twitter.com/FedorovMykhailo/status/
1497642156076511233

（10） Fendorf, Kyle. “The Dynamics of the Ukrainian IT Army’s Campaign in Russia.” *LAWFARE,* Lawfare Institute, 15 June 2023, https://www.lawfareblog.com/dynamics-ukrainian-it-armys-campaign-russia.

（11） 小泉悠「ウクライナ危機にみるロシアの介入戦略」『国際問題』六五八号、二〇一七年一月、三八頁、https://www2.jiia.or.jp/kokusaimondai_archive/2010/2017-01_005.pdf?noprint。

（12） Hoffman, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars.* Potomac Institute for Policy Studies, 2007, p. 28, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

（13） 稲垣芳朗「2014 年クリミア併合過程におけるハイブリッド戦の考察」『海幹校戦略研究』一二巻一号、二〇二二年六月、https://www.mod.go.jp/msdf/navcol/assets/pdf/ssg2022_06_03.pdf。

（14） Edelman, Eric S. “The Pros and Cons of‘Deterrence by Disclosure’.” *The Dispatch*, 21 February 2022, https://thedispatch.com/article/the-pros-and-cons-of-deterrence-by/.

（15） Sonne, Paul, et al. "Russian troop movements near Ukraine border prompt concern in U.S., Europe." *The Washington Post*, 30 October 2021, https://www.washingtonpost.com/world/russian-troop-movements-near-ukraine-border-prompt-concern-in-us-europe/2021/10/30/c122e57c-3983-11ec-9662-399cfa75efee_story.html.

（16） Harris, Shane, and Paul Sonne. "Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns." *The Washington Post*, 3 December 2021, https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html.

（17） US Department of State. *Secretary Antony J. Blinken at a Press Availability*. 7 January 2022, https://www.state.gov/secretary-antony-j-blinken-at-a-press-availability-11/.

（18） The White House. *Remarks by President Biden Providing an Update on Russia and Ukraine.* 18 February 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/18/remarks-by-president-biden-providing-an-update-on-russia-and-ukraine-2/.

（19） Soldatkin, Vladimir. "More than 10,000 Russian troops returning to bases after drills near Ukraine -Interfax." *Reuters,* 25 December 2021, https://www.reuters.com/markets/europe/more-than-10000-russian-troops-returning-bases-after-drills-near-ukraine-2021-12-25/.

（20） The Ministry of Foreign Affairs of the Russian Federation. "Foreign Minister Sergey Lavrov's working meeting with President of the Russian Federation Vladimir Putin, Moscow, February 14, 2022." 14 February 2022,https://mid.ru/en/foreign_policy/news/1798349/.

（21） "Zelensky hastily fled Kiev, Russian State Duma Speaker claims." *TASS,* 26 February 2022, https://tass.com/politics/1411855.

（22） ゼレンスキー大統領によるフェイスブック投稿 https://www.facebook.com/watch/?v=624877852076446

（23） ゼレンスキー大統領国外脱出との偽情報を発信したイラン国営英語ニュースチャンネル「Press TV」のX（旧ツイッター）投稿 https://twitter.com/PressTV/status/1499910982935715843

（24） ディスインフォメーションについては、筆者が提言作成を担った、笹川平和財団 政策提言「"外国からのディスインフォメーションに備えを！～サイバー空間の情報操作の脅威～"」二〇二二年二月、https://www.spf.org/security/publications/20220207_cyber.html を参照。

（25） Microsoft. "An overview of Russia's cyberattack activity in Ukraine." *Special Report: Ukraine,* 27 April 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

（26） Ibid. Microsoft, *Special Report: Ukraine,* p. 5.

（27） Ibid. Microsoft, *Special Report: Ukraine,* p. 6.

（28） Microsoft. *Defending Ukraine: Early Lessons from the Cyber War.* 22 June 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

（29） Ibid. Microsoft, *Special Report: Ukraine,* p. 7.

（30） Microsoft Digital Security Unit, et al. “Destructive malware targeting Ukrainian organizations.” *Microsoft Security Blog,* Microsoft, 15 January 2022, https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

（31） Microsoft Threat Intelligence.“Cadet Blizzard emerges as a novel and distinct Russian threat actor.” *Microsoft Security Blog,* Microsoft, 24 June 2023, https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/.

（32） CSIRT MON（ポーランド国防省コンピューター事案対応チーム）.“ANALYSIS OF THE CYBERATTACK ON UKRAINIAN GOVERNMENT RESOURCES.” 22 January 2022, https://csirt-mon.wp.mil.pl/pl/articles/6-aktualnosci/analysis-cyberattack-ukrainian-government-resources/.

（33） Hopkins, Valerie.“ A hack of the Defense Ministry, army and state banks was the largest of its kind in Ukraine’s history.” *The New York Times*, 15 February 2022, https://www.nytimes.com/2022/02/15/world/europe/ukraine-cyberattack.html.

（34） Ibid. Microsoft, *Special Report: Ukraine,* p. 7.

（35） Ibid. Microsoft, *Special Report: Ukraine,* p. 7.

（36） Ibid. Microsoft, *Special Report: Ukraine,* p. 12.

（37） Ibid. Microsoft, *Defending Ukraine*, pp. 7-9.

（38） Microsoft Threat Intelligence. “New “Prestigeransomware” impacts organizations in Ukraine and Poland.” *Microsoft Security Blog,* Microsoft, 14 October 2022, https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.

（39） Burt, Tom. “Malware attacks targeting Ukraine government.” *Microsoft On the Issues,* Microsoft, 15 January 2022, https://blogs.microsoft.com/on-the-issues/2022/01/15/mstic-malware-cyberattacks-ukraine-government/.

（40） Ibid. Microsoft, *Defending Ukraine*, p. 9.

（41） OneTrust DataGuidance. *Ukraine: Parliament passes draft law on cloud services.* 18 February 2022, https://www.dataguidance.com/news/ukraine-parliament-passes-draft-law-cloud-services.

（42） Viasat. *KA-SAT Network cyber attack overview.* 30 March 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

（43） Willuhn, Marian.“Satellite cyber attack paralyzes 11GW of German wind turbines.” *pv*

magazine, pv magazine group, 1 March 2022, https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/.

（44） NETBLOCKS. *Internet disruptions registered as Russia moves in on Ukraine.* 24 February 2022, https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K.

（45） 福島康仁「宇宙領域からみたロシア・ウクライナ戦争」高橋杉雄編著『ウクライナ戦争はなぜ終わらないのか―デジタル時代の総力戦―』文春新書、二〇二三年、一〇七～一四三頁参照。

（46） 小泉悠「ロシアのGPSスプーフィング能力」日本国際問題研究所『ポスト・プーチンのロシアの展望』二〇二〇年、七九～八九頁。

（47） HawkEye360. *HawkEye 360 Signal Detection Reveals GPS Interference in Ukraine.* Cision, 4 March 2022, https://www.prnewswire.com/news-releases/hawkeye-360-signal-detection-reveals-gps-interference-in-ukraine-301495696.html.

（48） “Russia Expands GPS Signal Jamming to 15 Regions.” *The Moscow Times,* 5 May 2023, https://www.themoscowtimes.com/2023/05/05/russia-expands-gps-signal-jamming-to-15-regions-a81049.

（49） 宮嶋茂樹『ウクライナ戦記―不肖・宮嶋 最後の戦場―』文藝春秋、二〇二二年、二〇三～二二〇頁。

（50） ＤＪＩ社ウェブサイト https://www.dji.com/jp/d-rtk/info

（51） Davenport, Christian. “Commercial satellites test the rules of war in Russia-Ukraine conflict. ” *The Washington Post*, 10 March 2022, https://www.washingtonpost.com/technology/2022/03/10/commercial-satellites-ukraine-russia-intelligence/.

（52） Antoniuk, Daryna. “Ukrainian charity buys satellite for the army. How will it help fight against Russia? ” T*he Kyiv Independent*, 27 August 2022, https://kyivindependent.com/ukrainian-charity-buys-satellite-for-the-army-how-will-it-help-fight-against-russia/.

（53） Ibid. 福島。

（54） Dastin, Jeffrey.“Ukraine is using Palantir’s software for ‘targeting,’ CEO says.” *Reuters*, 2 February 2023, https://jp.reuters.com/article/ukraine-crisis-palantir-idCAKBN2UC01O.

（55） Ibid. Davenport.

（56） フェドロフ副首相兼デジタル化担当大臣Ｘ（旧ツイッター）投稿 https://twitter.com/FedorovMykhailo/status/1497543633293266944

（57） マスク氏Ｘ（旧ツイッター）投稿 https://twitter.com/elonmusk/status/1497701484003213317

（58） Ibid. 宮嶋。

（59） Parker, Charlie.“Uber-style technology helped Ukraine to destroy Russian battalion.” *The Times*, 14 May 2022, https://www.thetimes.co.uk/article/uk-assisted-uber-style-technology-helped-ukraine-to-destroy-russian-battalion-5pxnh6m9p.

（60） ウクライナ国防省X（旧ツイッター）投稿 https://twitter.com/DefenceU/status/1524438980191731717

（61） Hammes, T.X. “Game-changers: Implications of the Russo-Ukraine war for the future of ground warfare.” *Issue Brief,* Atlantic Council, 3 April 2023, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/game-changers-implications-of-the-russo-ukraine-war-for-the-future-of-ground-warfare/.

（62） 詳しくは、大澤淳「新領域における戦い方の将来像―ロシア・ウクライナ戦争から見るハイブリッド戦争の新局面―」高橋杉雄編著『ウクライナ戦争はなぜ終わらないのか―デジタル時代の総力戦―』文春新書、二〇二三年、一四五～一八〇頁参照。

一章二節

（1） ロシアとハイブリッド戦争に検討した議論として、廣瀬陽子『ハイブリッド戦争―ロシアの新しい国家戦略―』講談社現代新書、二〇二一年や、小泉悠『現代ロシアの軍事戦略』ちくま新書、二〇二一年、および、大澤淳「主戦場となるサイバー空間 〝専守防衛〟では日本を守れない」『Wedge』三三巻一二号、二〇二一年一二月、二四～二七頁参照。

（2） Ibid. 小泉、六〇頁。

（3） Mattis, James N., and Frank G. Hoffman. “Future Warfare: The Rise of Hybrid Wars.” *Proceedings*, USNI, November 2005, https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars.

（4） Headquarters Department of the Army. *FM 3-0, Operations*. February 2008, https://army.rotc.umich.edu/public/resources/FM3-0Operations(FEB08).pdf.

（5） Krekel, Bryan, et al. *Capability of the People☒fs Republic of China to Conduct Cyber Warfare and Computer Network Exploitation: Prepared for The US-China Economic and Security Review Commission*. 9 October 2009, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

（6） US Department of Defense. *Quadrennial Defense Review Report*. February 2010, https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf.

（7） Käihkö, Ilmari. “The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession.” *The US Army War College Quarterly: Parameters*, US Army War College, vol. 51, no. 3, 25 August 2021, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3084&context=parameters.

（8） NATO. *Wales Summit Declaration*. 5 September 2014, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede240914walessummit_/sede240914walessummit_en.pdf.

（9） ロシアの現代戦コンセプトとハイブリッド戦概念については、Clark, Mason.“Russian Hybrid Warfare.”*Military Learning and The Future of War Series*, ISW, September 2020, https://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf.

（10） ロシア軍の現代戦コンセプトについては、佐々木孝博『近未来戦の核心サイバー戦―情報大国ロシアの全貌―』育鵬社、二〇二一年参照。

（11） *Герасимов B.B.* Ценность науки в предвидении.Новые вызовы требуют переосмыслить формы и способы ведения боевых действий //Военно-промышленный курьер, 2013, No.8 (476).

（12） これをゲラシモフ・ドクトリンと呼ぶか否かについては議論があるため、本稿ではコンセプトとした。

（13） ロシアの反射コントロールについては、Vasara, Antti.“Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy.” *Finnish Defence Studies*, no. 22, 2020, https://www.doria.fi/bitstream/handle/10024/176978/Vasara_FDS22_Theory%20of%20Reflexive%20Control%20%28web1%29-1.pdf?sequence=3&isAllowed=y.

（14） 笹川平和財団「外国からのディスインフォメーションに備えを！～サイバー空間の情報操作の脅威～」二〇二二年二月、五頁参照。https://www.spf.org/global-data/user172/cyber_security_2021_web1.pdf

（15） 大澤淳「主戦場となるサイバー空間 〝専守防衛〟では日本を守れない」『Wedge』三三巻一二号、二〇二一年一二月、二四～二七頁参照。

一章三節

（1） 内閣府総合科学技術・イノベーション会議「第 5 期科学技術基本計画」二〇一六年一月二二日閣議決定。

（2） NATO. “ Topics: NATO ’ s response to hybrid threats. ” 8 August 2019, https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en.

（3） NATO. “ The Secretary General ’ s Annual Report 2019. ” 19 March 2020, p. 29, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf.

（4） コンステレーションとは、「もともと『星座』を意味する言葉であるが、人工衛星の分野では全地球規模で人工衛星を多数機配置したシステムを指す。」齋藤宏文「宇宙研発、小型レ

ーダ衛星の多数機コンステレーション」JAXA 宇宙科学研究所、二〇一九年二月二六日、http://www.isas.jaxa.jp/feature/forefront/190226.html。

（5） Amies, Nick. “NATO includes threat of cyber attack in new strategic concept document.” *Deutsche Welle,* 14 October 2010, https://www.dw.com/en/nato-includes-threat-of-cyber-attack-in-new-strategic-concept-document/a-6072197.

（6） NATO. “The Secretary General’s Annual Report 2019.” 19 March 2020, p. 31, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf.

（7） U.S. Department of Defense.“Transcript: Secretary of Defense Lloyd J. Austin III Interview With Bret Baier, Fox News, at 2021 Reagan National Defense Forum.” 4 December 2021, https://www.defense.gov/News/Transcripts/Transcript/Article/2862114/secretary-of-defense-lloyd-j-austin-iii-interview-with-bret-baier-fox-news-at-2/.

（8） NATO. “News: NATO Secretary General discusses COVID-19 and disinformation with Lithuanian President.” 6 May 2020, https://www.nato.int/cps/en/natohq/news_175595.htm.

（9） Von Clausewitz, Carl. *On War*, ed. and trans. by Michael Howard and Peter Paret, Princeton University Press, 1984, P. 87.

（10） Singer, P. W., and Emerson T. Brooking. “What Clausewitz Can Teach Us About War on Social Media.” *Foreign Affairs,* 4 October 2018, https://www.foreignaffairs.com/articles/2018-10-04/what-clausewitz-can-teach-us-about-war-social-media.

（11） “Ukraine conflict: Putin 'was ready for nuclear alert’.” *BBC News,* BBC, 15 March 2015, https://www.bbc.com/news/world-europe-31899680.

（12） ジョージア侵攻は二〇〇八年八月八日から開始され、八月一二日に停戦が成立した。また、クリミア併合では二〇一四年二月二七日から三月二日の軍事作戦でクリミア半島占領が達成された。Herbst, John E., and Alina Polyakova. *Remembering the Day Russia Invaded Ukraine.* Atlantic Council, 24 February 2016, https://www.atlanticcouncil.org/blogs/ukrainealert/remembering-the-day-russia-invaded-ukraine/.

（13） Rühle, Michael. “Deterrence: what it can （and cannot） do.” *NATO Review,* NATO, 20 April 2015, https://www.nato.int/docu/review/articles/2015/04/20/deterrence-what-it-can-and-cannot-do/index.html.

（14） NATO. “Topics: Countering hybrid threats.” 8 August 2019, https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en.

（15） Rid, Thomas. “Cyberwar and Peace: Hacking Can Reduce Real-World Violence.” *Foreign Affairs,* 1 November 2013, https://www.foreignaffairs.com/articles/2013-11-01/cyberwar-and-peace.

（16）　川口貴久「米国におけるサイバー抑止政策の刷新―アトリビューションとレジリエンス」『Keio SFC Journal』一五巻二号、二〇一五年、https://gakkai.sfc.keio.ac.jp/journal/.assets/SFCJ15-2-04.pdf。

（17）　Gill, Bates, and Martin Kleiber. “China’s Space Odyssey: What the Antisatellite Test Reveals About Decision-Making in Beijing.” *Foreign Affairs,* 1 May 2007, https://www.foreignaffairs.com/articles/china/2007-05-01/chinas-space-odyssey-what-antisatellite-test-reveals-about-decision.

（18）　Colby, Elbridge. *FROM SANCTUARY TO BATTLEFIELD: A Framework for a U.S. Defense and Deterrence Strategy for Space.* Center for a New American Security, January 2016, p. 7, https://www.files.ethz.ch/isn/195913/CNAS%20Space%20Report_16107.pdf.

（19）　防衛省『令和２年版防衛白書』二〇二〇年、一二頁。

（20）　外務省「日米安全保障協議委員会（「２＋２」閣僚会合）の開催」二〇一一年六月、https://www.mofa.go.jp/mofaj/area/usa/hosho/2plus2_gai1106.html。

（21）　外務省「日米安全保障協議委員会（日米「２＋２」）」二〇一九年四月一九日、https://www.mofa.go.jp/mofaj/na/st/page4_004913.html。

（22）　The White House. Interim National Security Strategic Guidance. 3 March 2021, pp. 9-10, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

（23）　防衛省「日米安全保障協議委員会（２＋２）共同発表（仮訳）」https://www.mod.go.jp/j/approach/anpo/kyougi/2021/0316b_usa-j.html。

二章一節

（1）　operational domain と legal domain をそれぞれ作戦領域と法的領域と表記しても構わないのであるが、法的領域というと法と非法の内の一方を指すかなり大きな区分にも聞こえることから、本稿では領域とせず、両者ともにそのままドメインと記す。

（2）　ハーグ陸戦条約前文に置かれ、第一追加議定書第一条第二項で再確認されたもので、条約の明文規定がなくとも文民および戦闘員は文明国間に存立する慣習、人道の法則および公共良心の要求より生じる国際法の諸原則の保護と支配の下にあることをいう。核兵器の合法性に関する国際司法裁判所の勧告的意見では、条約が軍事技術の急速な発展に追随できずに生じる空隙を埋めて基本的保護を確保する機能をマルテンス条項が持つとされた。*Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996*, para. 78.

（3）　国際人道法は禁止規範の集合体であるとし、「禁止されないことは許される」の原則が今日も妥当して国際人道法からは行動の自由が確保されるとしても、平時一元化の現代では平時法からする禁止が重畳的にあり得る。国際人道法が禁止規範集合体か否かについてはさしあたり以下を見よ。Quintin, Anne. *The Nature of International Humanitarian Law: A Permissive or Restrictive Regime?* Edward Elgar Pub., 2020.

（4）　真山全「憲法的要請による集団的自衛権限定的行使の発現形態―外国領水掃海および

外国軍後方支援―」『国際問題』六四八号、二〇一六年、二三～二四頁。

（5）　したがって、一九五三年七月以降の南北朝鮮の軍事衝突は、平和条約締結前の朝鮮戦争休戦期間におけるそれであるからといって朝鮮戦争の一部となると認識することはできない。二〇一〇年の韓国海軍コルベット天安の北朝鮮軍による撃沈も朝鮮戦争とは別個の武力紛争とされ、国際刑事裁判所（ICC）検察局もそのように扱った。ICC Office of the Prosecutor. *Situation in the Republic of Korea: Article 5 Report*. Sec.54ff., 2014; 黒﨑将広他『防衛実務国際法』弘文堂、二〇二一年、二九八頁。

（6）　国際法関係文献で珍しくグレーゾーンに言及するものとしてアメリカ海軍大学校教官らによる Newport Manual on the Law of Naval Warfare（*International Law Studies*, Vol. 101（2023）, para. 2.1.2.1, p. 22）があるが、これとて法的状態としてグレーゾーンを扱ってはいない。

（7）　他にも一国の政府とそれが交戦団体承認を与えた反徒との闘争、および政府と自決権行使団体の間の闘争は国際的武力紛争である。

（8）　反徒同士の武力紛争や、国外にある非国家的主体と国家の間の武力紛争も非国際的武力紛争とされる。

（9）　もっとも、いくらかのハーグ法規則の非国際的武力紛争への適用を認める規定を設ける条約もある。特定通常兵器使用禁止制限条約（CCW）はその一例である（第一条第二項）。また、旧ユーゴスラヴィア国際刑事裁判所のいくつかの判決を機に、国際的と非国際的の武力紛争の規則を同一化する動きが目立つようになった。ICC 規程にもハーグ法の非国際的武力紛争適用を前提とする規定が交じる（第八条第二項（e）（ix）、（x）、（xii）～（xviii））。

（10）　台湾は住民、領域および政府の存在という国家三要件を満たしているものの、中国一国論から完全には脱しておらず、台北の政府はそれが中華民国という国号で呼んできた中国国家を代表する政府ではなく台湾という別国家の政府とは公然と言い切ってはいない。別国家であることを明言すれば中国の侵攻を招くからであるとはいえ、自ら国家であることを明確にしない実体の国家性は疑わしく、この状況を前提とすれば中台武力紛争を国際人道法からして直ちに国際的武力紛争であるというには躊躇する。台湾住民を自決権行使団体とすれば中台武力紛争を国際化できるともされるが、自決権行使団体たることが肯定されても、台湾が中国に制圧され第一追加議定書第一条第四項の本来的適用事態が生じるまでは武力紛争は国際的のそれにはならないと反論されるかもしれない。侵攻を受けてしまえば、国家に至らない自決権行使団体としての地位を主張するよりは国家性を主張した方が得策である。

台湾が覚悟を決めて国家性を明言すれば、台湾からして中台武力紛争は国際的のそれに転換される。他方、中国は台湾の国家性を引き続き否定しようから、中国から見れば中台紛争は非国際的武力紛争であることを変えず、中国が台湾軍構成員に捕虜資格を付与し、それとの戦闘にハーグ法を適用するとしてもそれは任意的にそうするのであって義務的であるからではないということになる。

ユス・アド・ベルムからしても国家性の公然たる表明のない限り問題は残り、非国家的主体を

集団的自衛権で助けることはコソボの場合と同じくできない。台湾が中国国家の一部を構成するという北京政府の主張を日米などが理解し尊重し、あるいはそれを認識（acknowledge）するというのは台湾問題平和的解決が前提であるというのではあるが、台湾による国家性の表明を欠いたままでは、中国が台湾に侵攻してこの前提が崩壊すれば台湾の国家性が自動的に認められるというわけにはいかないと思われる。いわゆる分裂国家の場合のそのそれぞれの側による自衛権行使を認めるという特殊な見解をとらない限りは、アメリカが台湾を集団的自衛権で支援するには、台湾の国家性が独立の宣明などで確認されなければならない。日本がそれ以前に台湾支援のアメリカ軍を日本が日米安保条約に従い支援することはできず、また台湾のために集団的自衛権を行使することも難しい。

（11）　同条の「如何ナル手段ニ依ルモ」は空対地攻撃でも地対地攻撃と同じ規則が適用されることを確認するために挿入されたとされる。*See*, Hanke, Heinz Marcus. “The 1923 Hague Rules of Air Warfare: A Contribution to the Development of International Law Protecting Civilians from Air Attack.” *International Review of the Red Cross*, no. 292, 1993, pp. 12-13.

（12）　*Ibid.*, pp. 12-44; Veuthey, Michel. “Histoire du droit international humanitaire dans la guerre aérienne.” Millet-Devalle, Anne-Sophie, ed. *Guerre aérienne et droit international humanitaire*. A. Pedone, 2015, pp. 37-68.

（13）　国際法における類推の分析については以下を見よ。Vöneky, Silja. “Analogy in International Law.” *Max Planck Encyclopedias of International Law*, 2008, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1375?print=pdf.

（14）　“A Declaration of the Independence of Cyberspace”（by John Perry Barlow, 1996, reproduced in *Duke Law and Technology Review*, vol. 18, 2019, pp. 5-7）なるものを含む独自性の主張に関する国際人道法からの分析として、Mačák, Kubo.“Silent War: Applicability of the *Jus in Bello* to Military Space Operations.”（*International Law Studies*, vol. 94, 2018, pp. 13-15）がある。

（15）　Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War*. Cambridge University Press, 2012, p. 28.

（16）　本稿では、武力紛争中のサイバー活動従事者が戦闘員資格保持を要求されるかの問題は扱わない。それは、電子戦を含む他の全ての敵対行為従事者の場合と基本的に変わらないからである。サイバー活動従事者の地位に関する最近の論稿として以下がある。茂木隆宏「サイバー空間における防御行為の武力紛争法上の評価」『同志社法学』七四巻六号、二〇二二年、三三三～四二四頁。この問題を検討するに際しては、敵対行為に参加した文民の捕虜資格が原則的には否定され、場合によっては背信行為として刑事責任を追及されることがあるとしても、文民の敵対行為参加それ自体を明示に禁止する規則は見当たらないことに留意を要す。禁止されない行為であっても、その従事者が後に法的責任を追及される場合が国際人道法にはある。

（17）　宇宙戦法規が新法的ドメインとなるかの検討の前に、宇宙条約などの平時の宇宙法に

より国際人道法適用が排除されないことの確認が必要であるが、ここでは国際人道法の適用はあるものとして議論を行う。

（18）　軍はこれまで少数の軍民の通信衛星や警戒衛星に依存していたため、これらの破壊や機能麻痺によって作戦行動に深刻な影響が生じることが懸念されていた。しかし、多数の衛星を低軌道で運用するようになったため、衛星の脆弱性は低下したともいわれる。衛星攻撃に関して法的検討を行う邦語論文として以下がある。青木節子「宇宙資産に対するサイバー攻撃に適用可能な国際法の検討」『国際法外交雑誌』一一五巻四号、二〇一七年、三五七〜三八〇頁、石井由梨佳「国際的武力紛争における軌道上人工衛星の保護」同、一二二巻一号、二〇二三年、四八〜七五頁。

（19）　*E.g.*, Steer, Cassandra. “Avoiding Legal Black Holes: International Humanitarian Law Applied to Conflicts in Outer Space.” *Proceedings of the 58th (2015) Colloquium on the Law of Outer Space*, October 2015.

（20）　Jakhu, Ram S., and Steven Freeland, eds. *McGill Manual on International Law Applicable to Military Uses of Outer Space*. McGill University, 2022; University of Adelaide. *The Woomera Manual on the International Law of Military Space Operations*. 2018, https://law.adelaide.edu.au/woomera/system/files/docs/Woomera%20Manual.pdf. マニュアル方式はサイバー活動についても用いられた。Schmitt, Michael, ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Oxford University Press, 2nd ed., 2017. 『タリン・マニュアル』の邦語解説については以下を見よ。中谷和弘、河野桂子、黒﨑将広『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、二〇一八年。マニュアルやガイドラインは現行法を取り込んでいる部分も少なくなく、新作戦ドメインに対する既存法的ドメインの支配を確認している箇所もある。また、法形成を誘導しようとする部分も認められる。マニュアルそれ自体は形式的法源ではないが、国家の作成するそれであれば当該国家の法意識の表明として一定の意味を持つ。

（21）　核爆発の場合には放射能汚染の評価が必要になり、民用物と区別される自然環境の損害はどう考えたらよいかの問題が生じる。ここでは議論を単純化するため、宇宙空間核爆発による放射能汚染は地上には及んでいないこととする。

（22）　第一追加議定書締約国ではないアメリカも、同議定書起草過程において核兵器使用への適用を否定する了解が成立していたと認識している。 US Department of Defense. *Law of War Manual*. Lieber and Sons, 3rd ed., 2017, para. 19.20, n. 201.

（23）　真山全「武力紛争法における『核の忘却』の終焉―対ウクライナ核攻撃を武力紛争法からどのように・どこまで非難できるか―」『有斐閣オンライン・ロージャーナル』（二〇二三年）（YOLJ-L2306008）、三三〜三五項、https://yuhikaku.com/articles/-/12925。

（24）　第一追加議定書第四九条第三項からして軍事目標の定義や予防措置などに関する規定を含む同議定書第四編第一部の宇宙空間への適用はない。石井、前掲注（18）、五一〜五二頁。しかし、この第四九条第三項は地上の文民に影響を与える海空戦への同部適用は認めるので、同

項のいう「空戦」に宇宙での戦いが解釈上含まれ得るかが問題になる。

二章二節

（1）　オーガスト・ベクエイ『コンピュータ犯罪との戦い』奥山甚一・吉成哲信訳、工学社、一九八〇年（原著 Bequai, August. *Computer Crime*. Lexington Books, 1978）。著者はかなり早い時期から、経済犯罪やコンピューター犯罪を取り扱った論文を数多く発表しており、インターネット上の弁護士情報ウェブサイトなどによると、現在もバージニア州にて弁護士として活動中とのことであるが、現在専門とする分野は異なるようである。

（2）　本稿においては、コンピューターとコンピューターシステムへの侵入、乗っ取りなどの行為を、便宜上「ハッキング」と記すこととする。便宜上、というのは、「クラッキング」という用語の方が正確に意を伝えることができるのではないか、という説得的な議論があることは認識している一方、「ハッキング」という用語の方が、より広く使用されていると思われるためである。

（3）　サイバー空間で展開される「攻撃」または「害意のある行動」については、「サイバーテロ」、「サイバー攻撃」、「サイバー戦（争）」などいろいろな言葉が使われるが、法律的な観点からは厳密な定義を意識して使用されるべきものも多いので、本稿では最も不正確のそしりを逃れやすいであろう「サイバー攻撃」を、包括的概念を示すものとして使用している。

（4）　「サイバー空間」も、いわば「何となく」使用されることが多い外来語であるため、念のため語意を確認しておくと、「サイバー空間、またはサイバースペースとは、主にコンピュータやネットワークによって構築された仮想的な空間を指します。現在であれば、インターネットが代表的なサイバー空間だと言えます。」（NTT コミュニケーションズ「サイバー空間とは」『ICT Business Online』 https://www.ntt.com/bizon/glossary/j-s/cyber-kukan.html）といったあたりが標準的な理解であろうか。アメリカ国立標準技術研究所（NIST）による定義もほぼ同様の記述となっている。（“A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” 〈“cyberspace” *COMPUTER SECURITY RESOURCE CENTER,* NIST, https://csrc.nist.gov/glossary/term/cyberspace.〉）

（5）　ここに述べた前線と銃後とをはっきり区別することが困難となるという事態は、実はサイバー空間の出現以前にも観察されている。二〇世紀の二度にわたる世界大戦の時期に航空戦力が実用化され、それによって特に文民の居住地域や工業地帯などに対する戦略爆撃が行われるようになったために、そのような区別が困難となる事態が現出したことを想起されたい。

（6）　本書においては、第一章、特にその第二節において、ハイブリッド戦の定義や態様について詳述されているので、ハイブリッド戦に関する詳細かつ包括的な説明についてはそこに譲ることとしたい。

（7）　防衛省・自衛隊「第一章一、現在の安全保障環境の特徴」『令和 4 年版防衛白書』 二

〇二二年、https://www.mod.go.jp/j/press/wp/wp2022/html/n110001000.html。

（8） Jordan, Javier. “International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict.” *Journal of Strategic Security,* vol. 14, no. 1, 2020, pp. 1-24 at 2.

（9） Carment, David and Dani Belo.“War’s Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare.” *Policy Paper,* Canadian Global Affairs Institute, October 2018, at 2.

（10） Hoffman, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies, December 2007, at 14. 引用部分の訳は筆者による。

（11） 慶応義塾大学の廣瀬陽子教授は、ロシアにおいてもハイブリッド戦概念が存在する一方、ハイブリッド戦（Гибридная война）という言葉自体はあまり使用されないと指摘している。廣瀬陽子『ハイブリッド戦争―ロシアの新しい国家戦略―』講談社現代新書、二〇二一年、三二頁。

（12） Carment and Belo, *supra* note 9.

（13） Carment and Belo, *supra* note 9.

（14） 起訴状の例として、U.S. v. Wang Dong et al. (*See*, https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf)、U.S. v. Wu Zhiyong et al. (*See*, https://www.justice.gov/d9/press-releases/attachments/2020/02/10/wu_zhiyong_indictment.pdf)などがある。これらの事件は、いずれも中国人民解放軍の構成員がアメリカに存在するコンピューターシステムに侵入し情報を窃取した、という事実関係から複数の罪名でアメリカにおいて起訴されたものである。

（15） 近年の例を含めパブリック・アトリビューションを紹介したものとして、公安調査庁『サイバー空間における脅威の概況 2022』二〇二二年、九頁以下。

（16） パブリック・アトリビューションの概念自体も、論者によりその射程が異なるが、本稿においては紙幅の関係もあり、そういった議論があることを指摘するにとどめる。瀬戸崇志「国家のサイバー攻撃とパブリック・アトリビューション：ファイブ・アイズ諸国のアトリビューション連合と SolarWinds 事案対応」『NIDS コメンタリー』一七九号、防衛研究所、二〇二一年七月一五日、http://www.nids.mod.go.jp/publication/commentary/pdf/commentary179.pdf。

（17） あえてくだけた韻を踏んだ表現であり、「名指しをすることで恥をかかせる」というのが直訳である。

（18） Kaushik, Anushka. “Public attribution and its scope and efficacy as a policy tool in cyberspace.” *Digital Frontiers,* Observer Research Foundation, 21 October 2019, https://www.orfonline.org/expert-speak/public-attribution-and-its-scope-and-efficacy-as-a-policy-tool-in-cyberspace-56826/.

（19） *Id.*

（20） *See generally*, Schweichler, Steven R. “Generating a Global Cyber Code of Conduct.” *USAWC Civilian Research Project,* US Army War College, 1 April 2011,

https://apps.dtic.mil/sti/pdfs/ADA565251.pdf; McCarthy, Thomas, and Alison Russell. “Roadmap for a Code of Conduct for Cyberspace.” *Fletcher Security Review,* vol. 2, no. 2, September 2015, pp. 1-7.

（21） Oh, Lionel. “The Bifurcation of International Cyber Norms: Navigating the Space In-Between.” *Singapore Policy Journal,* HKS Student Journals, 26 January 2021, https://spj.hkspublications.org/2021/01/26/the-bifurcation-of-international-cyber-norms-navigating-the-space-in-between/; Dawda, Suneha. “Competing for the Middle Ground in Internet Governance.” *Commentary,* The Royal United Services Institute for Defence and Security Studies, 22 June 2022, https://rusi.org/explore-our-research/publications/commentary/competing-middle-ground-internet-governance. また、ロシア・ウクライナ戦争開戦後に、サイバー・ガバナンスを超えて、より広い視野でこの二極化を論じたものとして、Lewis, James Andrew. *Global Governance after Ukraine.* Center for Strategic and International
Studies, 1 March 2022, https://www.csis.org/analysis/global-governance-after-ukraine.

（22） 法律事務所に対するサイバー攻撃のうち被害が顕著であったものを中心に紹介したものとして、Arctic Wolf. *The Top 10 Legal Industry Cyber Attacks.* Arctic Wolf Networks Inc., 20 July 2023, https://arcticwolf.com/resources/blog/top-legal-industry-cyber-attacks/.

（23） *Securities and Exchange Commission v. Iat Hong et al.* , NO. 16-CV-9947 (S.D.N.Y. filed Dec. 27, 2016)(https://www.sec.gov/litigation/litreleases/lr-23826) “ Manhattan U.S. Attorney Announces Arrest Of Macau Resident And Unsealing Of Charges Against Three Individuals For Insider Trading Based On Information Hacked From Prominent U.S. Law Firms.” *US Attorney’s Office - Southern District of New York,* US Department of Justice, 27 December 2016, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-arrest-macau-resident-and-unsealing-charges-against; Security and Exchange Commission. “Chinese Traders Charged With Trading on Hacked Nonpublic Information Stolen From Two Law Firms.” *Securities and Exchange Commission online,* 27 December 2016, https://www.sec.gov/news/press-release/2016-280.

（24） いささか旧聞に属するが、 国家情報長官、およびCIA、国家安全保障局（NSA）、国防情報局（DIA）、連邦捜査局（FBI）、国家地理空間情報局（NGA）の各長官が出席した上院の公聴会の記録が、この問題の全体像を理解するのに参考になる。“Open Hearing on Worldwide Threats, Hearing Before the Select Committee on Intelligence of the United States Senate, Senate Hrg, 115-278, 115th Congress, 2nd Session.” *U.S. Government Information,* U.S. Government Publishing Office, 13 February 2018, full transcript available at https://www.govinfo.gov/content/pkg/CHRG-115shrg28947/pdf/CHRG-115shrg28947.pdf.

（25） 土屋大洋「米国におけるサイバーセキュリティ政策」『米国内政と外交における新展開』日本国際問題研究所、二〇一三年三月、一三五頁；出口雅史「サイバー攻撃に対する制裁の考察

―オバマ政権の対朝、対中、対露制裁を中心に―」『中央大学社会科学研究所年報』二三号、二〇一九年九月、二九〇頁。

（26） Sekara, Hunter. “A Look at the Computer Security Act of 1987.” *TripWire Blog,* Fortra, 1 December 2020, https://www.tripwire.com/state-of-security/computer-security-act-of-1987; 同法とその関連情報については、“H.R. 145 - Computer Security Act of 1987. ” *Congress.GOV,* Library of Congress, https://www.congress.gov/bill/100th-congress/house-bill/145/text. を参照。

（27） “PDD-63 - Critical Infrastructure Protection.” Clinton Digital Library, 20 May 1998, https://clinton.presidentiallibraries.us/items/show/12762.

（28） 土屋、*supra* note 25、一三六頁。出口、*supra* note 25、二九〇～二九一頁。

（29） *Defending America’s Cyberspace - National Plan for Information Systems Protection.* Version1.0, The White House, January 2000, https://clintonwhitehouse4.archives.gov/media/pdf/npisp-execsummary-000105.pdf.

（30） 土屋、*supra* note 25、一三六頁。出口、*supra* note 25、二九一頁。

（31） *The National Strategy to Secure Cyberspace.* The White House, February 2003, https://nsarchive.gwu.edu/sites/default/files/documents/2700096/Document-16.pdf.

（32） 出口、*supra* note 25、二九二～二九三頁。

（33） *The International Strategy for Cyberspace - Prosperity, Security and Openness in a Networked World.* The White House, May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

（34） “The Department of Defense Strategy for Operating in Cyberspace.” The Department of Defense, July 2011, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

（35） Office of the Press Secretary. *Presidential Policy Directive - Critical Infrastructure Security and Resilience (PPD-21).* The White House, 12 February 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

（36） Office of the Press Secretary. *Improving Critical Infrastructure Cybersecurity (Executive Order 13636).* The White House, 12 February 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

（37） これまで、PPP には「官民連携」という訳語をあててきているが、ここも含め本稿のいくつかの場所では「協働」という言葉もあてている。これは、ＰＰＰに含まれる “partnership” の語の語感を日本語に訳すことが難しいことによる。管見するところ、日本語における「連携」に比べると、当事者お互いに対する関与の度合いがより深いように感じられる PPP の運用もあ

ると思われるため、「連携」と「協働」の語が併用されていること、ご容赦いただければと願うものである。

（38） The Department of Homeland Security. *National Infrastructure Protection Plan 2013 -Partnering for Critical Infrastructure Security and Resilience.* Cybersecurity & Infrastructure Security Agency, 2013, https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf.

（39） *Critical Infrastructure Partnership Advisory Council (CIPAC).* Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/resources-tools/groups/critical-infrastructure-partnership-advisory-council-cipac.

（40） *Sector Coordinating Councils.* Cybersecurity & Infrastructure security Agency, https://www.cisa.gov/resources-tools/groups/sector-coordinating-councils.

（41） “S.2519 - National Cybersecurity Protection Act of 2014.” *Congress.Gov,* Library of Congress, https://www.congress.gov/bill/113th-congress/senate-bill/2519.

（42） “S.754 - Cybersecurity Information Sharing Act (CISA).” *Congress.Gov,* Library of Congress, https://www.congress.gov/bill/114th-congress/senate-bill/754.

（43） 岩崎海「経済安全保障　重要インフラにおけるサイバーセキュリティに関する情報共有の在り方　セキュリティ・クリアランスを視点に」日本総合研究所、二〇二三年四月三日、https://www.jri.co.jp/page.jsp?id=104879。

（44） 政府の秘密情報が漏えいすることによる不利益を防ぐために、秘密情報を取り扱う人物等を事前に審査する仕組み（岩崎海「企業向け　経済安全保障におけるセキュリティクリアランスの活かし方」日本総研、二〇二二年六月二日、https://www.jri.co.jp/page.jsp?id=102813）

（45） 筆者による仮訳。原語は “National Cybersecurity and Communications Integration Center”.

（46） *National Cyber Strategy of the United States of America.* The White House, September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

（47） *National Security Strategy of the United States of America.* The White House, December 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

（48） 「柱」の意。

（49） Inzaurralde, Bastien. “The Cybersecurity 202: Trump administration seeks to project tougher stance in cyberspace with new strategy.” *The Washington Post,* 21 September 2018, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/21/the-cybersecurity-202-trump-administration-seeks-to-project-tougher-stance-in-cyberspace-with-new-strategy/5ba3e85d1b326b7c8a8d158a/.

（50） Atkinson, Wade H. Jr.“A Review of the Trump Administration’s National Cyber

Strategy: Need for Renewal and Rethinking of the Public-Private Partnership in U.S. National Security Policy." *Active Measures,* The Institute of World Politics, 22 October 2020, https://www.iwp.edu/active-measures/2020/10/22/a-review-of-the-trump-administrations-national-cyber-strategy-need-for-renewal-and-rethinking-of-the-public-private-partnership-in-u-s-national-security-policy/.

（51） "Cybersecurity and Infrastructure Security Agency Act of 2018, H.R. 3359, Pub.L. 115-278." *U.S. Government Information,* U.S. Government Publishing Office, 16 November 2018, https://www.govinfo.gov/content/pkg/PLAW-115publ278/pdf/PLAW-115publ278.pdf.

（52） Nakashima, Ellen. "White House authorizes'offensive cyber operations' to deter foreign adversaries." *The Washington Post,* 20 September 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html. Nakashima 記者の取材によると、"offensive cyber operations"とは、国際法上武力の行使に当たらないものをいう、とのことである。同覚書は機密文書指定がなされており、内容については公表されていない。Smalley, Suzanne. "Biden administration is studying whether to scale back Trump-era cyber authorities at DOD." *CYBERSCOOP,* Scoop News Group, 31 March 2022, https://cyberscoop.com/biden-trump-nspm-13-presidential-memo-cyber-command-white-house/.

（53） *Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems*. The White House, 4 September 2020, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.

（54） *The Artemis Accords.* National Aeronautics and Space Administration, 13 October 2020, https://assets.publishing.service.gov.uk/media/5f8726f8d3bf7f6334bd0599/Artemis_Accords_signed_13Oct2020_002_.pdf.

（55） *Executive Order on Improving the Nation's Cybersecurity.* The White House, 12 May 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

（56） *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems.* The White House, 28 July 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

（57） *National Cybersecurity Strategy.* The White House, 1 March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

（58）　田中絵麻、齋藤孝道「米国におけるサイバーセキュリティエコシステムの構成要素と政策展開」『明治大学国際日本学研究』一三巻一号、二〇二〇年、七七～九三頁。

（59）　英語では通常“civil-military relationship”と「民」の方が先に言及されるが、日本語では「軍民」と呼びならわしているものと思われるので、あえて「民軍」とはしなかった。

（60）　Shulman, Mark R.“Support and Defend: Civil-Military Relations in the Age of Obama.” *Fordham International Law Journal,* vol. 35, 2012.

（61）　Ackerman, Bruce. *The Decline and Fall of the American Republic.* Belknap Press, 2010. Ackerman と Mazur（*infra* note 62）の議論については、Shulman が手際よくまとめている通りである（*supra* note 60）が、ここで若干脱線することをお許し頂きたい。Shulman が述べる（*Id.* at p. 427）通り、Ackerman の手になる本書のタイトルは、かのエドワード・ギボンの『ローマ帝国衰亡史（*The History of the Decline and Fall of the Roman Empire*）』を意識したものであろうし、Ackerman 自身が本書の導入部分において、Arthur M. Schlesinger の *The Imperial Presidency*（複数の出版社から出版されているが、筆者は、Mariner Books による二〇〇四年出版のペーパーバックを参照した）に言及しつつ一九七〇年代以降の大統領について述べるあたり（*see e.g.* Ackerman, *supra*, at p. 5）にも、現在のアメリカの政治状況を古代ローマのそれ、特に共和制から帝政への移行期に重ねて議論していることは明らかであろう。もちろん、アメリカを古代ローマ帝国になぞらえる論者が、枚挙にいとまがないことは言うまでもない。Ackerman が“…the fall of the *Republic* is compatible with the continuation of American *empire*…”（*see, e.g., Id.,* at p. 10, 強調は筆者）と述べるあたり、アメリカ政治上の言説において“Republic”が背負う意味、そしてなぜ Republic が大文字で始まる固有名詞で、empire はそうではないのか、といったところを理解することが大切であろうことが痛感される。“republic”が「共和国」と訳されたことにより捨象されてしまった、*res publica* の語源的味わいの部分を十分に言語化する努力が追い付かないまま、自らの浅学を常日頃恥じている筆者としては、これらも、機会を得て十分に分析を試みたいと考えているアメリカ史の底流につながっているように感じられる。

（62）　Mazur, Diane H. *A More Perfect Military: How the Constitution Can Make Our Military Stronger.* Oxford University Press, 2010.

（63）　*supra* note 60, pp. 424-426.

（64）　*See* e.g., *Id.* pp. 422-426.

（65）　*Id.* p. 414.

（66）　*Id.* pp. 442-444.

（67）　ここで紹介したような軍民関係論は極論ではないかと思われる向きもあるかもしれないので、たとえば、もう一つの戦略産業分野と広く考えられているバイオ分野においても、類似の動きがあることを指摘しておきたい。保健福祉省の一部局に、災害やその他の公衆衛生上の緊急事態に対する対応をその任務とする戦略的準備・対応管理局（ASPR：Administration for Strategic Preparedness and Response）というものがあり、さらにその一部門として生物医学先

端研究開発局（BARDA：Biomedical Advanced Research and Development Authority）がある。BARDA は①化学物質、生物、放射性物質、または核物質による事故、事件や攻撃、または②広域インフルエンザや新種の感染症など、によって生ずる緊急事態に対応するためのワクチン、薬品、療法、診断法を統合的組織的に開発する方法を提供することをその任務とする。そしてBARDA はその任務の遂行にあたり、民間のパートナー企業と協働することができるシステムとなっており、このような任務を付与されているため、BARDA の開発プロジェクトは、安全保障上の脅威となる疫学的または医学的な問題に対する解決策を、民間企業と共に開発するというものとなっているものがほとんどである（*See generally*, https://aspr.hhs.gov/AboutASPR/ProgramOffices/BARDA/Pages/Doing-Business-with-BARDA.aspx）。たとえば、二〇〇四年七月二一日に開始され現在も継続中である Project Bioshield においては、その目的は、研究、治験、製造と購買のための複数年にわたる資金供与を民間企業に行うことで、国家安全保障にとっての重要性の非常に高い脅威に対する医学的解決策を開発していくことである。国家安全保障のための民間企業の動員というコンセプトは、ここにもみられるといえよう（https://aspr.hhs.gov/AboutASPR/ProgramOffices/BARDA/Pages/Project-Bioshield.aspx）。

（68） *See generally*, 林紘一郎、田川義博「サイバー攻撃の被害者である民間企業の対抗手段はどこまで可能か：日米比較を軸に」『情報セキュリティ総合科学』一〇号、二〇一八年一一月、https://www.iisec.ac.jp/proc/vol0010/hayashi-tagawa18.pdf。林と田川は「passive defense と offense 間のグレイ・ゾーンにある active cyber defense」（一頁）について積極的な論旨を展開するが、その過程でそれに伴う困難さも数多く的確に指摘する。

（69） Lobo-Guerrero, Luis. *Insuring War – Sovereignty, Security and Risk*. Routledge, 2012, p. 21. 一六五〇年代にロンドン市民の憩いの場として流行していたコーヒーハウスの一つを、エドワード・ロイドという人物がテムズ川沿いで始めたところ、そこに海運関係者が出入りするようになったのが、現在の保険市場または取引所としてのロイズ・オブ・ロンドンの源流である。初期ロイズにおける取引を活写したものとして、Herschaft, Jeremy A. “Not Your Average Coffee Shop: Lloyd’s of London – A Twenty-First-Century Primer on the History. Structure, and Future of the Backbone of Marine Insurance.” *Tulane Maritime Law Journal,* vol. 29, no. 2, Summer 2005.

（70） War and terrorism risk insurance, war and terrorism insurance, terrorism insurance などいろいろな呼称があるので、このように総称した。

（71） “H.R.3210 - Terrorism Risk Insurance Act of 2002.” *Congress.Gov,* Library of Congress, https://www.congress.gov/bill/107th-congress/house-bill/3210. 二〇〇二年制定、その後複数回の延長を経て、二〇一九年に二〇二七年まで延長されている。

（72） *Id. Section 102(1)(a)(ii).*

（73） Patel, Nehal. “Cyber and TRIA: Expanding the Definition of an“Act of Terrorismto” Include Cyber Attacks.” *Duke Law & Technology Review,* Duke University School of Law, vol.

19, February 2021, pp. 23-42, at 30.

（74） *Mondelez International, Inc. v. Zurich Insurance Company* , 2018 WL 4941760 (Ill.Cir.Ct., 2018) (Trial Pleading)

（75） *Merck v. Ace American Insurance Company* (475 N.J.Super. 420, 293 A.3d 535, 2023(2023))

（76） Martin, Alexander. "Mondelez and Zurich reach settlement in NotPetya cyberattack insurance suit." *The Record,* Recorded Future News, 31 October 2022, https://therecord.media/mondelez-and-zurich-reach-settlement-in-notpetya-cyberattack-insurance-suit.

（77） *Supra* note 75, at p.3. 該当箇所英文原文を以下に掲げる。

"1) Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack:

a) by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval or air forces;

b) or by military, naval, or air forces;

c) or by an agent of such government, power, authority or forces;

This policy does not insure against loss or damage caused by or resulting from Exclusions A., B., or C., regardless of any other cause or event contributing concurrently or in any other sequence to the loss."

（78） 文字通り邦訳すれば、「戦争除外条項」であるが、保険業界の用語としては「戦争免責条項」が一般的であるので、本稿においても「戦争免責条項」を用いる。

（79） *Supra* note 75, p. 8 *et seq.*

（80） *Id.* p. 6 *et seq.* このように、約款条項が複数の解釈を許すものであった場合、それは、約款を準備した当事者である保険者に対して厳格に解釈される、とする法理を *contra proferentem* の法理という。

（81） テロ、戦争、金融危機のような社会経済的リスクは、人為的あるいは政治的原因で巨大な規模の損害が発生し得るため保険の対象とすることが難しいとされる。堀田一吉『現代リスクと保険理論』東洋経済新報社、二〇一四年。

（82） Patel, *supra* note 73, at pp. 24-26.

（83） Webel, Baird. "The Terrorism Risk Insurance Act (TRIA)" *Congressional Research Service,* Library of Congress, updated 10 February 2022, https://crsreports.congress.gov/product/pdf/IF/IF11090/5.

（84） Patel, *supra* note 73, p. 29 et seq.

（85） Abraham, Kenneth S., and Daniel Schwarcz. "Courting Disaster: The Underappreciated Risk of a Cyber Insurance Catastrophe." *Connecticut Insurance Law Journal,* vol. 27, no. 2, Spring 2021, pp. 407-473.

（86） Kashyap, Ashwin. “ Underestimating Volatility in the Cyber Insurance Market. ” *MarshMcLennan,* Marsh & McLennan Companies, Inc., https://www.marshmclennan.com/insights/publications/2018/sep/underestimating-volatility-in-the-cyber-insurance-market.html.

（87） “Terrorism Risk Insurance Act (TRIA).” *Center for Insurance Policy and Research,* National Association of Insurance Commissioners, last updated 26 January 2023, https://content.naic.org/cipr-topics/terrorism-risk-insurance-act-tria.

（88） たとえば、アメリカ・カリフォルニア州に本社のある Cowbell Cyber, Inc.（https://cowbell.insure/）は、顧客ベースを中小企業に特化した、“Adaptive Cyber Insurance”を提供している。（*Adaptive Cyber Insurance.* Cowbell Cyber Inc., September 2022, https://cowbell.insure/wp-content/uploads/2022/09/Cowbell-Adaptive-Cyber-Insurance.pdf ）これは、サイバーリスクに関するビッグデータを分析し、サイバー空間における脅威の状況や被保険者のリスクの状況などを頻繁にアップデートすることで、現在年度ごとに行われている保険約款の見直しをより頻繁に行い、適正な付保の条件を適時に設定していく、というものである。（Lunden, Ingrid.“Cowbell raises $100M to build out its AI-based cyber insurance platform for SMBs.” *TechCrunch,* Yahoo, 15 March 2022, https://techcrunch.com/2022/03/15/cowbell-raises-100m-to-build-out-its-ai-based-cyber-insurance-platform-for-smbs/.)。イングリッド・ルンデン氏のこの記事は、同社の革新的なアプローチについて簡潔な要約を行っている。

（89） *See, e.g. supra* note 57, *National Cybersecurity Strategy*. そこで多用される“digital ecosystem”、“human prosperity”といった語が、どのような文脈で使用されているかに注目したい。

（90） Luttwak, Edward N.“Toward Post-Heroic Warfare.” *Foreign Affairs*, vol. 74, no. 3, May/June 1995, pp. 109-122.

三章一節

（1） 大澤淳「認知領域に対する情報操作型サイバー攻撃（情報戦）の脅威―民主主義を脅かすディスインフォメーション―」『治安フォーラム』二八巻一一号、二〇二二年九月、四九～五八頁。

（2） 以下の記述は下記による。佐藤謙、大澤淳「激化するサイバー戦に無力の日本 法と体制整備を急げ」『Wedge』三四巻八号、二〇二二年八月、四三～四五頁。

（3） NATOサイバー防衛センターが公表した、サイバー攻撃に関する国際法のルールについて国際法学者や実務家によりまとめられた学説集。英語原文は Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017。本書では、日本語訳（中谷和弘、河野桂子、黒﨑将広『サイバー攻撃の国際法―タリン・マニュアル２・０の解説【増補版】―』信山社、二〇二三年）から引用し、三六五頁の参考資料に本文で引用している各規則を掲載している。

（4）　“18 U.S. Code Chapter 119 - WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS.” *Legal Information Institute*, Cornell Law School, https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119.

三章二節

（1）　「例えば、米国や欧州、わが国などが自由なサイバー空間の維持を訴える一方、ロシアや中国、新興国などの多くは、サイバー空間の国家管理の強化を訴えている。」防衛省『令和 4 年度版防衛白書』二〇二二年、一七二頁。

（2）　対象とするサーバーやウェブサイトに大量のデータを送り付け、過剰な負荷をかけてシステムを使用不能にするサイバー攻撃

（3）　感染すると端末などに保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラム

（4）　インターネット上の IP アドレスとドメイン名を対応付ける DNS（Domain Name System）を誤作動させる攻撃

（5）　マルウェア（悪意を持ったプログラム）を感染させデータの削除やシステムの破壊によりサーバーやパソコンを使用不能にする攻撃

（6）　Microsoft. *Defending Ukraine: Early Lessons from the Cyber War*. 22 June 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

（7）　ロシア・ウクライナ戦争で最初に使用されたのは「ハーメティック・ワイパー（Hermetic Wiper）」と呼ばれ、システムの完全な破壊を狙ったもの

（8）　サーバーなどのハードウェア、アプリケーションなどのソフトウェアを使用者の管理する施設内に設置して運用すること

（9）　クラウドの標準的なサービスを不特定多数が共同で利用する形態

（10）　パソコンやサーバーなどの端末をコンピューターウイルスなどのマルウェア感染から保護すること

（11）　Microsoft. *Defending Ukraine: Early Lessons from the Cyber War*. 22 June 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

（12）　行為主体の特定を困難にし、自らの行為の正当化や情報のかく乱に重きを置いた情報戦

（13）　攻撃者がシステムに侵入するために、管理者に気づかれないように設置した侵入口のこと（ESET「バックドアを利用したサイバー攻撃の仕組みと事例」『サイバーセキュリティ情報局』二〇二〇年八月二五日、https://eset-info.canon-its.jp/malware_info/special/detail/200825.html）

（14）　SNS などを通じた「三戦」（心理戦、輿論戦、法律戦）や偽情報の散布などによって一般市民の心理を操作・かく乱し、社会の混乱を生み出そうとすること

（15）　物理領域や情報領域におけるさまざまな活動を通じて、心理・認知領域に影響を与え、意思決定に影響を与える、主に国家主体による活動

（16）　社会、公益への攻撃を目的とした害意のある情報

（17）　国防動員体制の整備に加え、緊急事態に限られない平素からの民間資源の軍事利用や、軍事技術の民間転用などを推進するもの

（18）　Binding Operational Directive 23-01 - Improving Asset Visibility and Vulnerability Detection on Federal Networks

（19）　国民保護法第三二条に基づき策定された「国民の保護に関する基本指針」（二〇〇五年三月二五日閣議決定）において示された武力攻撃事態四類型および緊急対処事態二類型（および例示）にもサイバー攻撃は含まれていない。

（20）　このために必要な機能として「攻撃者が悪用するサーバの探知のための情報収集」「攻撃を防ぐための手段」「サイバー・インテリジェンス収集分析」「民間セクターのインシデント調査・支援・対処調整」「官民情報共有等の連携強化」が掲げてある。

（21）　第一九六回国会衆議院安全保障委員会議録第三号、二〇一八年三月二二日、七頁、小野寺五典防衛大臣答弁

（22）　内閣参質二一〇第八二号、二〇二二年一二月二三日

（ 𝔖 ）　USCYBERCOM. *U.S. Cyber Command 2022 Year in Review*. 30 December 2022, https://www.cybercom.mil/Media/News/Article/3256645/us-cyber-command-2022-year-in-review/.は「二〇二二年一月中旬にロシアが壊滅的な被害を与える可能性のあったサイバー攻撃を開始したとき、ウクライナのサイバー専門家は HFOs チームと共に、危害が及ぶ前に悪意のあるサイバー活動を混乱または停止することができた」と報告している。

（24）　OS やアプリケーションで発見された問題点や脆弱性に対し、これらの不具合を解消するための追加プログラム

三章三節

（1）　US Department of Defense. *Department of Defense Cyber Strategy 2018 Summary*. September 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

（2）　大澤淳「迫り来るサイバー攻撃の脅威―ハイブリッド戦争と日本への影響―」『治安フォーラム』二八巻六号、二〇二二年五月、四二～五一頁。

（3）　大澤淳「ランサムウェアの脅威―サイバー犯罪を装うロシアによるランサムウェア攻撃―」『治安フォーラム』二八巻七号、二〇二二年六月、五七～六八頁。

（4）　大澤淳「情報窃取型サイバー攻撃の脅威―国の競争力を奪う中国による標的型攻撃―」『治安フォーラム』二八巻九号、二〇二二年八月、五八～六七頁。

（5）　大澤淳「北朝鮮のサイバー攻撃の脅威―外貨獲得を狙う金銭目的型サイバー攻撃―」『治安フォーラム』二八巻一〇号、二〇二二年九月、六一～六九頁。

（6）　アメリカの第五世代戦闘機 F-22 や F-35 の技術情報がサイバー攻撃によって中国に流出し、中国空軍の J-31 戦闘機に用いられた事例がある。

（7）　中国軍と密接な関係にあるサイバー攻撃グループ APT1 は、アメリカの原子力、太陽光、鉄鋼、非鉄金属企業から技術を窃取したことが知られている。

（∞）　FireEye. "APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat." *Mandiant*, 6 April 2017, https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html.

（9）　内閣官房経済安全保障法制準備室「経済安全保障法制に関する有識者会議」資料、二〇二一年一一月二六日。

（10）　大澤淳「認知領域に対する情報操作型サイバー攻撃（情報戦）の脅威―民主主義を脅かすディスインフォメーション―」『治安フォーラム』二八巻一一号、二〇二二年一〇月、四九～五八頁。

（11）　Jasper, Scott. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. Rowman & Littlefield Publishers, 2017, p. 18.

（12）　US Department of Defense. *The DoD Cyber Strategy*. April 2015, https://nsarchive.gwu.edu/sites/default/files/documents/2692133/Document-25.pdf.

（13）　Owens, William A., et al., eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. National Academies Press, 2009.

（14）　US Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. July 2011.

（15）　"Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats." *Center for Cyber and Homeland Security*, George Washington University, 2016, https://cynergia.mx/wp-content/uploads/2016/12/CCHS-ActiveDefenseReportFINAL.pdf.

（16）　White House. *National Cyber Strategy of the United States of America*. September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

（17）　合衆国法典 18 U.S.C. § 1345 (a) (1) (A).

（18）　US Department of Justice. "U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage." *US Attorney's Office for the Western District of Pennsylvania*, 19 May 2014, https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and.

（19）　UK Government. *National Cyber Security Strategy 2016-2021*. March 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/

file/567242/national_cyber_security_strategy_2016.pdf.

（20）　大澤淳「国家を背景としたサイバー脅威への対処―積極的サイバー防御の導入に向けて―」『治安フォーラム』二八巻一二号、二〇二二年一一月、六一～六九頁。

（21）　サイバーセキュリティ戦略本部「サイバーセキュリティ戦略」二〇一八年七月二七日、https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf。

（22）　Ibid., p. 20.

三章四節

（1）　「国家安全保障戦略」二〇二二年一二月、Ⅵ2（4）ア（傍点は筆者による）。

（2）　「国家防衛戦略」二〇二二年一二月、Ⅲ3。

（3）　*Brussels Summit Communiqué*. 14 June 2021, Para. 32, https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en.

（4）　Bundesministerium des Innern, *Cyber-Sicherheitsstrategie für Deutschland 2016*, S. 5, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/cybersicherheitsstrategie-2016.pdf;jsessionid=37376CDA16255A659EAAE5DA2FCB1849.1_cid373?__blob=publicationFile&v=4.

（5）　Die Bundesregierung, *Weissbuch 2016 -Zur Sicherheitspolitik und zur Zukunft der Bundeswehr*. S. 38, https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf.

（6）　ドイツの再軍備と緊急事態条項導入のための憲法改正の概要については、参照、松浦一夫『立憲主義と安全保障法制―同盟戦略に対応するドイツ連邦憲法裁判所の判例法形成―』三和書籍、二〇一六年、三～二〇頁。

（7）　以下、ワイマール憲法とドイツ基本法の日本語訳については、参照、高田 敏・初宿正典編訳『ドイツ憲法集〔第８版〕』信山社、二〇二〇年。ただし、ドイツ基本法の防衛関連条文の邦訳については、前掲拙著、四七六～四九五頁。ドイツ基本法の最新のドイツ語原文および英語訳文は、以下の URL を参照。ドイツ語原文：https://www.gesetze-im-internet.de/gg/BJNR000010949.html 、英語訳文：https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html

（8）　左派党議員の質問主意書「『サイバー空間』における戦争」[BT-Drucks.18/6496]第二問に対する二〇一五年一二月一〇日付政府答弁書の回答[BT-Drucks.18/6989, S.4.]。

（9）　この論点に関するドイツ憲法学説について、詳しくは、松浦一夫「ドイツにおけるサイバー安全保障と防衛憲法」『憲法研究』五四号、二〇二二年六月、一～二八頁参照。以下の説明は、主にこの論文に依拠する。

（10）　松浦一夫「9・11 米国テロ事件以後のドイツ政府の対応と政策課題」『防衛法研究』二

六号、二〇〇二年一〇月、五五頁。

（11）　NATO 域外派兵をめぐる憲法裁判と議会関与法制定の経緯について、参照、前掲拙著、第一部および第三部。

（12）　前出の左派党議員による質問主意書第三六問および第三七問に対する政府答弁書の回答[BT-Drucks.18/6989, S.12f.]。

（13）　防衛出動による対応は「存立危機事態」の場合にも考えられる。同事態の認定要件は、「我が国と密接な関係にある他国」に対する武力攻撃が発生し、これにより日本国の存立が脅かされ、国民の生命・自由などが根底から覆される明白な危険があることであり、「武力攻撃事態」よりいっそう複雑な判断になる。反面、日本と「密接な関係にある」諸国とのサイバー攻撃に関する情報共有とこれへの共同対処の契機ともなり得ることは重視すべきである。

（14）　一九七三年九月二三日、参議院本会議、山中防衛庁長官答弁、また、田村重信『新・防衛法制』内外出版、二〇一八年、一六九頁以下参照。

（15）　「洞爺湖サミット 航空テロ撃墜検討」『読売新聞』二〇〇八年一月二四日、一面。

（16）　ドイツにおける政府の情報活動とその議会による統制について、参照、渡邉斉志「ドイツ「信書、郵便及び電信電話の秘密の制限のための法律」の改訂」『外国の立法』二一七巻、二〇〇三年八月、一一五〜一三三頁、同「ドイツにおける議会による情報機関の統制」『外国の立法』二三〇巻、二〇〇六年一一月、一二四〜一三一頁、および、渡辺富久子「ドイツの連邦情報庁法―対外情報機関の活動の法的根拠―」『外国の立法』二七五巻、二〇一八年三月、五五〜八〇頁。

（17）　Die Bundesregierung, *Nationale Sicherheitsstrategie: Integrierte Sicherheit für Deutschland " Wehrhaft. Resilient. Nachhaltig "*, Juni 2023, S. 62.（ドイツ語原文：https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf 、英語訳文：https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf）

この文書では、ドイツ政府がサイバー攻撃に対してEUのパートナー国、NATOの同盟国、または他の関係諸国と共に攻撃の加害者を特定し制裁を行うことが宣言されると共に、国全体の抗堪性（レジリエンス）と国家の行動能力を維持するために、サイバー空間において常時対応・防御できるよう、「サイバーセキュリティ・アーキテクチャーをさらに発展させる」と記す。ドイツのサイバーセキュリティ・アーキテクチャーの詳細については、Herpig, Sven, et al. *Deutschlands staatliche Cybersicherheitsarchitektur*. 10. Auflage, Stiftung Neue Verantwortung, Mai 2023.（第一〇版ドイツ語原文：https://www.stiftung-nv.de/sites/default/files/cybersicherheitsarchitektur_zehnteauflage 1023.pdf 、第九版英語訳文：https://www.stiftung-nv.de/sites/default/files/9thed_cybersecurityarchitecture.pdf）

三章五節

（1）　原典は、Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law*

Applicable to Cyber Operations. Cambridge University Press, 2017。日本語版は、中谷和弘、河野桂子、黒﨑将広『サイバー攻撃の国際法―タリン・マニュアル 2・0 の解説【増補版】―』信山社、二〇二三年。

（2） "The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector." *The Oxford Process*, Oxford Institute for Law, Ethics and Armed Conflict, 2020, https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/he-oxford-statement-on-cyber-operations-targeting-the-health-care-sector/; *The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research*. Oxford Institute for Law, Ethics and Armed Conflict, 7 August 2020, https://www.elac.ox.ac.uk/the-second-oxford-statement-on-international-law-protections-of-the-healthcare-sector-during-covid-19-safeguarding-vaccine-research/.

（3） Schmitt, Michael N. "Three International Law Rules for Responding Effectively to Hostile Cyber Operations." *Just Security*, 13 July 2021, https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/.

（4） The Federal Government of Germany. *On the Application of International Law in Cyberspace*. March 2021, p. 14, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

（5） TM2, p. 318, Commentary, para. 19. 『サイバー攻撃の国際法』八二頁。

（6） Milanovic, Marko, and Michael N. Schmitt. "Cyber Attacks and Cyber （Mis）information Operations During a Pandemic." *Journal of National Security Law & Policy*, vol. 11, 2020, p. 258, https://jnslp.com/wp-content/uploads/2020/12/Cyber-Attacks-and-Cyber-Misinformation-Operations-During-a-Pandemic_2.pdf.

（7） The UK Government. *International Law in Future Frontiers*. 19 May 2022, https://www.gov.uk/government/speeches/international-law-in-future-frontiers.

（8） TM2, p. 20, Commentary, para. 10 et seq.『サイバー攻撃の国際法』規則四の解説参照、一八頁。

（9） TM2, p. 22, Commentary, para. 16.

（10） カナダ政府は「本質的な政府の機能」として医療の他、法執行、選挙、税の徴収、国防、外交を挙げている。Government of Canada. *International Law applicable in cyberspace*. April 2022, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng.

四章一節

（1） Silverstein, Benjamin, and Ankit Panda. *Space Is a Great Commons. It□fs Time to Treat It as Such*. Carnegie Endowment for International Peace, 9 March 2021, https://carnegieendowment.org/2021/03/09/space-is-great-commons.-it-s-time-to-treat-it-as-such-pub-84018.

（2） United Nations. *General Assembly: Outer Space Increasingly ' Congested, Contested and Competitive', First Committee Told, as Speakers Urge Legally Binding Document to Prevent Its Militarization*. 25 October 2013, https://www.un.org/press/en/2013/gadis3487.doc.htm.

（3） Bahney, Benjamin, and Jonathan Pearl. *Why Creating a Space Force Changes Nothing: Space Has Been Militarized From the Start*. Foreign Affairs, 26 March 2019, https://www.foreignaffairs.com/articles/space/2019-03-26/why-creating-space-force-changes-nothing.

（4） 福島康仁『宇宙と安全保障―軍事利用の潮流とガバナンスの模索―』千倉書房、二〇二〇年、一〇五頁。

（5） Colby, Elbridge. *FROM SANCTUARY TO BATTLEFIELD: A Framework for a U.S. Defense and Deterrence Strategy for Space*. Center for a New American Security, January 2016, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Space-Report_16107.pdf.

（6） The White House. *President Donald J. Trump is Unveiling an America First National Space Strategy*. 23 March 20
18, https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/.

（7） GIS Arta は、ドローン、アメリカおよびNATOの情報フィード、従来の前方監視員から目標情報を取得し、その情報を砲兵用の正確な座標に変換する、OS「アンドロイド」用のアプリを指す（*GIS "ARTA": Automated Command and Control System*. https://gisarta.org/en/.）。

（8） Missiroli, Antonio. "Game of drones? How new technologies affect deterrence, defence and security." *NATO Review*, NATO, 5 May 2020, https://www.nato.int/docu/review/articles/2020/05/05/game-of-drones-how-new-technologies-affect-deterrence-defence-and-security/index.html.

（9） NATO. " Emerging and disruptive technologies. " 22 June 2023, https://www.nato.int/cps/en/natohq/topics_184303.htm.

（10） Schmitt, Michael, and Kieran Tinkler. *War in Space: How International Humanitarian Law Might Apply*. Just Security, 6 March 2020,

https://www.justsecurity.org/68906/war-in-space-how-international-humanitarian-law-might-apply/.

（11） McFall, Caitlin. “Russia threatens to target Western commercial satellites like Elon Musk ’ s Starlink. ” *Fox News*, FOX News Channel, 27 October 2022, https://www.foxnews.com/world/russia-threatens-target-western-commercial-satellites-elon-musks-starlink.

（12） White House. *Press Gaggle by Press Secretary Karine Jean-Pierre En Route Syracuse, NY*. 27 October 2022, https://www.whitehouse.gov/briefing-room/press-briefings/2022/10/27/press-gaggle-by-press-secretary-karine-jean-pierre-en-route-syracuse-ny/.

（13） Corera, Gordon. “Russia hacked Ukrainian satellite communications, officials believe.” *BBC News*, BBC, 25 March 2022, https://www.bbc.com/news/technology-60796079.

（14） Page, Carly. “US, UK and EU blame Russia for‘unacceptable’ Viasat cyberattack.” *TechCrunch*, Yahoo, 10 May 2022, https://techcrunch.com/2022/05/10/russia-viasat-cyberattack/.

（15） 軍縮会議日本政府代表部「宇宙空間における軍事・安全保障面での制度的枠組み」二〇二三年四月一一日、https://www.disarm.emb-japan.go.jp/itpr_ja/chap12.html。

（16） 「日米安保条約 5 条、北方領土・竹島は適用外 加藤官房長官が見解」『産経新聞』二〇二〇年一一月一二日、https://www.sankei.com/article/20201112-V2EZ2GNPVRPLDPDABBKDS75WRA/。

（17） NATO. *Pre-ministerial press conference by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Defence Ministers*. 11 October 2022, https://www.nato.int/cps/en/natohq/opinions_208037.htm.

四章二節

（1） US Department of Defense. *Quadrennial Defense Review 2014*. March 2014, https://www.acq.osd.mil/ncbdp/docs/2014_Quadrennial_Defense_Review.pdf.

（2） US Department of Defense. *Defense Space Strategy: Summary*. June 2020, https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF.

（3） US Office of Space Commerce. *National Space Policy of the United States of America*. December 2020, https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/12/National-Space-Policy.pdf.

（4） 内閣官房「国家安全保障戦略について」二〇一三年一二月、https://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-j.pdf。

（5） 宇宙開発戦略本部「宇宙基本計画」二〇一五年一月、

https://www8.cao.go.jp/space/plan/plan2/plan2.pdf。

（6）　内閣官房「宇宙基本計画の変更について」二〇二〇年六月、https://www8.cao.go.jp/space/plan/kaitei_fy02/fy02.pdf。

（7）　自由民主党政務調査会「小型衛星コンステレーション時代への対応と民の力を引き出す挑戦的な政策の推進―第七次提言―」二〇二一年五月、https://www.shindo.gr.jp/cms/wp-content/uploads/2021/06/0601-2.pdf。

四章三節

（1）　Adamy, David. *Ew 101: A First Course in Electronic Warfare.* Artech House, 2001. 邦訳版（河東晴子他訳『電子戦の技術：基礎編』東京電機大学出版局、二〇一三年）四頁。

（2）　防衛省『令和 3 年度防衛白書』第Ⅲ部第 1 章第 3 節「電磁波領域での対応」https://www.mod.go.jp/j/pub
lication/wp/wp2021/html/n310303000.html

（3）　Ibid. Adamy, 一九二〜一九六頁。

（4）　防衛装備庁「研究開発ビジョン　電磁波領域の取組」二〇二〇年三月三一日、https://www.mod.go.jp/atla/soubiseisaku/vision/rd_vision_kaisetsuR0203_01.pdf。

（5）　Ibid. 防衛装備庁

五章一節

（1）　本書では便宜上、中大型の飛行機タイプのものを無人機（UAV）、マルチコプタータイプに代表される小型のものを小型ドローン、これらを総称し無人航空機と呼ぶ。

（2）　内閣官房「平成 31 年度以降に係る防衛計画の大綱について」二〇一八年一二月一八日、https://www.cas.go.jp/jp/siryou/pdf/h31boueikeikaku.pdf。

（3）　内閣官房「中期防衛力整備計画（平成 31 年度〜平成 35 年度）について」二〇一八年一二月一八日、https://www.cas.go.jp/jp/siryou/pdf/h3135cyuukiboueiryoku.pdf。

（4）　防衛省『令和 5 年度版防衛白書』二〇二三年、七三頁、https://www.mod.go.jp/j/press/wp/wp2023/pdf/R05zenpen.pdf。

（5）　内閣官房「国家安全保障戦略について」二〇二二年一二月一六日、https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf。内閣官房「国家防衛戦略について」二〇二二年一二月一六日、https://www.cas.go.jp/jp/siryou/221216anzenhoshou/boueisenryaki.pdf。内閣官房「防衛力整備計画について」二〇二二年一二月一六日、https://www.kantei.go.jp/jp/content/000120948.pdf。

五章二節

（1）　撃破、損傷、放棄、鹵獲。発表元によって約一七〇〇両（オランダの軍事情報サイト「Oryx」）から三二〇〇両以上（ウクライナ軍参謀本部）と大きく差がある。

（2）　「国家防衛戦略」一八頁、「防衛整備計画」四頁　（二〇二二年一二月閣議決定）

（3）　自衛隊法第百七条（航空法等の適用除外）第一項

（4）　「無人航空機の飛行に関する訓令」（防衛省訓令第五四号、二〇一五年一二月一〇日〈改正二〇二二年一二月一三日〉）

（5）　「陸上自衛隊の保有する無人航空機の運用基準について（通達）」（陸幕情第二〇号、二〇二三年二月一日）

（6）　多用途／攻撃用 UAV の運用実証：情報収集機能に加えて、火力及び電磁波による攻撃機能を効果的に保持した多用途 UAV、侵攻部隊等の情報を収集し、即時に火力発揮可能な攻撃用 UAV を取得し、運用実証を行う。

小型攻撃用 UAV の運用実証：島嶼等における着上陸侵攻対処及び重要施設等の防護に際して、侵攻部隊を探知・識別して人員、車両、舟艇等に対処できる小型攻撃用 UAV を取得し、運用実証を行う。

（防衛省『我が国の防衛と予算　令和五年度予算の概要』二〇二二年一二月、一八頁、https://www.mod.go.jp/j/budget/yosan_gaiyo/2023/yosan_20230328.pdf）

（7）　船舶自動識別装置（AIS）：一定の船舶に装備が義務付けられており、船名、船種、船位、針路、速度、仕向地、積載物などを自動的に送信する。

（8）　空中衝突防止装置（TCAS）：航空機の周囲を監視し、空中衝突の恐れがある他の航空機の存在を操縦士に警告する。

（9）　「科学若しくは技術の発達のための実験、電波の利用の効率性に関する試験又は電波の利用の需要に関する調査を行うために開設する無線局であつて、実用に供しないもの（電波法施行規則第四条第二十二項）」であり、周波数割当計画の周波数割当表に定める周波数にかかわらず周波数を割当てられる。

（10）　オプショナルな無人／有人艦（Optionally Manned Ship）：たとえば、平時においては任務に応じて乗員が乗り組んで行動し、有事における危険を伴う行動の場合は無人で運航するなど、「選択式」に運用できる艦艇。

（11）　空母打撃群（CSG：Carrier Strike Group）などによるパワープロジェクション（戦力投射）に先立ち、長距離攻撃兵器（艦対艦／艦対空ミサイル）を装備した小規模の小型艦艇、USV部隊が、戦域で分散して行動しつつも、ネットワークで連接され、一体化した索敵・攻撃能力として海上優勢を獲得する作戦。

（12）　対潜魚雷を格納した状態で海底に敷設され、敵潜水艦が近接したことを自己のセンサーが探知すると、対潜魚雷を発射する機雷。

五章三節

（1）　二〇二三年二月二七日の浜田防衛大臣記者会見。

（2）　Program on Humanitarian Policy and Conflict Research at Harvard University. *Manual on International Law Applicable to Air and Missile Warfare*. 15 May 2009.

（3）　Dinstein, Yoram, and Arne Willy Dahl. *Oslo Manual on Select Topics of the Law of Armed Conflict: Rule and Commentary*. Springer, 2020. 本マニュアルは、前述の『航空戦・ミサイル戦に適用される国際法マニュアル』を更新するために作成された、国際法研究者によるマニュアルである。これらのマニュアルは条約でなく、あくまで国際法研究者の見解にすぎず、法的拘束力はないが、国際法解釈において重要な参考資料となっている。

（4）　航空自衛隊保有の偵察用大型UAVグローバルホークは通常の円形の白地に赤の日の丸ではなく、ロービジ版（low visibility, 低視認性塗装）の円形の白地に灰色の日の丸が表示されている。

（5）　U.S. Navy. *The Commander⊠fs Handbook on the Law of Naval Operations* (*NWP 1-14 M*). March 2022.

（6）　ロシア・ウクライナ戦争では少なくとも二〇二二年一〇月二九日および二〇二三年五月二四日、二〇二三年七月一七日に自爆USV攻撃が発生している。

（7）　たとえば、一九二五年のジュネーヴ・ガス議定書は、戦時に化学兵器の使用を禁止したが、化学兵器の開発・製造は禁止しておらず、国際法上の復仇による化学兵器の使用を留保する国（アメリカ）もあった。復仇は、国際違法行為の中止や救済を求めるための被害国による一方的措置であり、それが違法行為であっても違法行為への対抗措置であるために、その違法性が阻却される。

（8）　文民への誤射・誤爆に関する上官責任に関して、指揮官が入手し、あるいは、入手すべき情報に基づいて攻撃が合法であると合理的に結論付けた場合、結果として均衡しない文民被害は発生したとしても、指揮官は刑事責任を負わない（「合理的指揮官」基準、通称「レンデュリック・ルール」）。

（9）　テロリスト殺害数と文民被害者数の比較衡量だけでなく、殺害対象が高価値の標的（高官・幹部）か否かも考慮する必要がある。標的が高官であり、その排除が敵対行為の早期終了をもたらすならば、多数の文民被害が発生しても、比例原則が満たされるかもしれないからである。区別原則と比例原則について、岩本誠吾「国際法における無人兵器の評価とその規制動向」『国際安全保障』四二巻二号、二〇一四年九月、一八〜一九頁。

（10）　突入自爆ドローンには、アメリカ製スイッチブレード 300 のような兵士がモニターで標的を確認しながら自爆攻撃させるカメラ映像遠隔操作型と、前記のハーピーのようなAIが標的を捜索して自爆攻撃させるパッシブレーダーホーミング式自律型の二種類がある。

（11）　二〇二一年三月八日の国連安保理リビア専門家パネル報告書（S/2021/229）が、LAWSの使用を暗示しているが、明確かつ詳細に記述しておらず、その存在は正式に確認されたとは言えない。

（12）　CCW Meeting of the High Contracting Parties. *Final Report* （*CCW/MSP/2013/10*). 16 December 2013, par. 32.

（13）　CCW Meeting of the High Contracting Parties. *Final Report* （*CCW/MSP/2013/10*). 13 December 2019, par. 32 and Annex Ⅲ

（14）　将来構想にある有人航空機と無人航空機の連携運用の中で、有人航空機操縦士が無人航空機搭載兵器を発射させることは、地上からの遠隔操作と同様に、人間の意思が介在していると言える。

（15）　ハード・ローは法的拘束力のある条約などの法規範を指し、他方、ソフト・ローは法的拘束力を持つに至っていない法形成途上の非法規範である。後者に法的意義がまったくないというわけではない。

（16）　政府専門家報告書（CCW/GGE.1/2023/2, 24 May 2023, Advance Version, par. 22）。運用期間の制限事例として、CCW 第二改正議定書での遠隔散布対人地雷は、三〇日以内の自己破壊装置および一二〇日以内の自己不活性化装置の装着が義務付けられている（技術的事項に関する附属書）。運用領域の制限事例として、CCW 第三議定書での空中投下の焼夷兵器は、人口周密地域での使用が禁じられている（第二条第二項）。

（17）　UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. SHS/BIO/PI/2021/1. 23 November 2021.

（18）　European Commission. *Proposal for a Regulation of the European Parliament and the Council laying Down Harmonised Rules on Artificial Intelligence*（*Artificial Intelligence Act*）*and Amending certain Union Legislative Acts*（*COM/2021/206 final*）. 21 April 2021. AIは、許容できないリスクのあるAI（禁止）、ハイリスクのあるAI（規制）、限定リスクのあるAI（透明性義務）、最小限リスクのあるAI（規制なし）の四つに類型化される。EUのAI規制案のような容認不可のAI利用禁止と条件付きのAI利用規制は、LAWS・AWSの二層アプローチと共通した規定構成となっている。

（19）　U.S. Department of Defense. *DOD Adopts Ethical Principles for Artificial Intelligence*. 24 February 2020. その倫理原則とは、責任性、衡平性、追跡可能性、信頼性、統制可能性である。