International Review of the Red Cross (2025), **107** (928), 311–334.
The Military
doi:10.1017/S181638312400047X

IRRC

US military legal doctrine and the emerging wartime cyber environment

Emily Bobenrieth[1,2]* and Sean Watts[3,4,5,6,7]†
[1]Judge Advocate, US Army
[2]Faculty, US Army Judge Advocate General's Legal Center and School, Charlottesville, VA, United States
[3]Professor, United States Military Academy, West Point, NY, United States
[4]Co-Director, Lieber Institute for Law and Warfare, West Point, NY, United States
[5]Co-Editor-in-Chief, Articles of War
[6]Co-General Editor, Lieber Studies Series, Oxford University Press, Oxford, UK
[7]Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
*Corresponding author email: emily.e.bobenrieth.mil@army.mil

Abstract

Newly emerging US cyberspace warfighting concepts highlight the need to update US legal doctrine. Concepts adapted to future high-intensity, high-paced armed conflict, including command post dispersal and integration of cyberspace into other targeting

† The views and opinions presented herein are those of the authors and do not necessarily represent the views of the US Department of Defense or US Army.

domains, present opportunities to refine US understandings of the law of war attack threshold and overlooked rules applicable to destruction and seizure. The advantages of staking out clear and current opinio juris *on these and other matters extend beyond providing responsible and consistent operational law advice. Updated and authoritative military cyber legal doctrine will serve the strategic and diplomatic legal interests of the United States and the international legal system as a whole.*

Keywords: law of war, law of armed conflict, international humanitarian law, cyber, multi-domain operations, command dispersal, attack, destruction, seizure, constant care.

> The challenge is not whether existing international law applies to cyberspace …. The challenge is providing decision makers with considerations that may be taken into account when determining how existing international law applies to cyber activities.[1]

Introduction

In November 2017, a new US military lawyer was deployed to an exercise designed to simulate large-scale combat operations against a near-peer adversary. Her unit's senior military attorneys were committed to operations elsewhere. As a result, and within a year of law school graduation, she served as the sole attorney advising the exercise-based combat operations of a Corps-level Joint Operations Center (JOC).[2] For three weeks, she monitored and advised on all operational activity in the Corps JOC across multiple domains of warfare, including the cyber domain.

That a junior military legal adviser would be called upon to advise at that level of command is extraordinary in the context of modern, law-saturated US military operations. While the exercise context explains the situation in significant part, these circumstances may closely resemble a new normal in tomorrow's wars. Anticipated increases in military sensing and targeting capabilities will place traditionally centralized command and control facilities and their large staffs at enormous, even intolerable risk.[3] Survival and success will

1 "United States Submission to the 2014–2015 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications", in CarrieLyn D. Guymon (ed.), *Digest of United States Practice in International Law*, Office of the Legal Adviser, US Department of State, 2015, p. 732.

2 A JOC is a centralized facility where military staff plan, coordinate and execute joint military actions and operations involving each service of the US Armed Forces. US Department of Defense (DoD), Joint Chiefs of Staff, *Joint Campaigns and Operations*, Joint Publication 3-0, 18 June 2022, p. GL-12.

3 Large-scale combat operations refer to "extensive joint combat operations in terms of scope and size of forces committed, conducted as a campaign aimed at achieving operational and strategic objectives." US Department of the Army, *Operations*, Army Publishing Directorate 3-0, July 2019, p. 1-5.

require smaller, highly dispersed command elements that exercise widely delegated authority across every domain of war.

Future large-scale combat operations will also afford reduced opportunities for the exhaustive coordination and staffing, including legal support, that have characterized twenty-first-century warfare. To survive and win, States' armed forces are likely to wrest control of strategic assets and their considerable effects from high-level, specialized organizations and disseminate them to lower, tactical-level units, commanders, and their staffs.[4] The dispersal and delegations that these developments require will have profound operational and legal implications for all domains of war,[5] but none more so than the cyber domain. Traditional models of command and control and legal oversight by large consolidated staff organizations may no longer be feasible or fit for purpose on the modern battlefield.

Simultaneously with dispersed command and authority delegation, US plans for near-future war envision significant integration of cyber operations into nearly every battlefield activity. Some of that near future is already unfolding in the ongoing conflicts in Ukraine and Gaza.[6] If previous practice had seen cyber operations and operators cloistered into national-level, domain-specific campaigns, ongoing military art and emerging US doctrine envision highly integrated and increasingly delegated cyber capabilities and operations. The Pentagon's shorthand for this integration and synchronization of its warfighting capabilities is "multi-domain operations", or in US military circles, MDO.[7] It envisions the complete and seamless fusion of warfighting capabilities and lines of effort, including cyber operations, into a unified and mutually supporting enterprise of targeting.

4 US doctrine describes three levels of warfare: strategic, operational and tactical. At the strategic level, national interests drive the employment of instruments of national power to allow the president to examine and account for an adversary's strategies as well as understand the evolving operating environment. The operational level of warfare links the tactical and strategic levels, conducting campaigns typically comprised of major military objectives. The tactical level involves individual battles, engagements and activities aimed at achieving a greater military objective. DoD, above note 2, pp. I-10–I-11.

5 The five operational domains are land, air, sea, space and cyberspace. US Department of the Army, *The U.S. Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1, December 2018, p. i.

6 The Pentagon has openly admitted to providing cyber defence assistance to Ukraine to counter Russian cyber attacks. Julian E. Barnes, "The Pentagon Says It Has Helped Ukraine Thwart Russian Cyberattacks", *New York Times*, 19 December 2022, available at: www.nytimes.com/2022/12/19/world/europe/ukraine-cyber-national-mission-force.html (all internet references were accessed in October 2024). Hacktivism has become a hallmark of the Ukrainian defensive strategy. Tim Starks, "Red Cross Officials Want Civilian Hackers to Follow Rules Amid War. Here's Why", *Washington Post*, 5 October 2023, available at: www.washingtonpost.com/politics/2023/10/05/red-cross-wants-civilian-hackers-follow-rules-heres-why. During the present war in Gaza, connections to communications and internet services have been unreliable at best, impeding families from communicating, as well as humanitarian relief organizations and non-governmental organizations from connecting with their personnel. Tom Bateman and Antoinette Radford, "People in Gaza Uncontactable and All Communication Down as Israel Intensifies Bombing", *BBC News*, 27 October 2023, available at: www.bbc.com/news/world-middle-east-67241362.

7 Multi-domain operations involve the combined arms employment of joint and Army capabilities through all available domains to accomplish the mission with effective combat power at the least cost. Multi-domain operations span across the conflict continuum. US Department of the Army, *Operations*, Field Manual 3-0, 1 October 2022, p. 1-2.

This turn from a centralized and specialized model of cyber planning and execution toward a generalist model with greater operational integration will see a parallel shift in supporting legal expertise. Legal support to wartime cyber operations will migrate in significant part from large staff sections of comparatively specialized military cyber lawyers to smaller cadres of generalist law of war practitioners. While diligent and trusted staff members, these generalist military lawyers bring comparatively lower degrees of familiarity, experience and facility with the policies and legal intricacies that have formed US military cyber law practice. More so than their specialist counterparts, they will require and benefit from clear legal policy guidance across the entire spectrum of wartime cyber operations that their units will carry out.

However, existing US military legal resources for wartime cyber operations are sparse. This is particularly true of law of war rules applicable to operations characterized as below the *jus in bello* threshold of attack. Personal and recent publicly available experience indicate that operations below the attack threshold account for a significant portion of cyber operations during armed conflict. While US legal doctrine in that realm is thin and ambiguous, academic and humanitarian communities offer refined and increasingly progressive legal schemes for law of war (and other) regulation of non-attack cyber operations. The task of applying these progressive, often avant-garde legal analyses to actual operations is difficult and highly fraught. The extent to which they reflect *lex lata* as understood by States, and particularly by the United States, is often unclear.

A survey of emerging US cyber warfighting concepts evaluated against rudimentary legal guidance developed nearly a decade ago makes clear the need for updated wartime cyber law doctrine. As cyber capabilities and operations proliferate and are further integrated into US military units' operational authority and organic capabilities, the advantages to staking out clear *opinio juris* on these matters extend beyond providing responsible and consistent operational law advice. Updated and authoritative military cyber legal doctrine will ensure effective planning and execution of US wartime cyber operations. It will also serve many strategic and diplomatic legal interests of the international legal system as a whole.

The cyber domain in armed conflict

The threats posed to States by cyber operations have been widely recognized since the turn of the last century. Meanwhile, cyber operations' simultaneous potential to be effective lines of effort in States' own campaigns is equally appreciated. In 1999, as a herald of the wartime role of cyber operations, the US Department of Defense (DoD) issued new legal guidance on information operations, including their cyber aspects.[8] By 2005, the DoD had formally recognized cyberspace as its fifth

8 DoD, *An Assessment of International Legal Issues in Information Operations*, 2nd ed., November 1999, available at: https://nsarchive.gwu.edu/document/21410-document-13.

operational domain alongside land, sea, air and space.[9] In 2009, the US secretary of defence merged two defence organizations to form the national-level US Cyber Command.[10] And in 2018, the US president elevated Cyber Command to a unified combatant command, completing in large part the evolution of cyber operations into a full-fledged US warfighting function.[11]

The United States' largest alliance structure has largely followed suit. While the North Atlantic Treaty Organization (NATO) did not formally designate cyberspace as an operational domain until 2016, it recognized the role that cyber operations play in its security far earlier.[12] At its Prague Summit in 2002, NATO first identified cyber operations as a threat to the alliance.[13] In 2008, it accredited the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia as a hub for cyber wargaming and research on the technical, policy and legal aspects of cyber operations.[14] And by 2014, NATO recognized cyber attacks as a basis for the invocation of its collective self-defence provision.[15]

Recognition of the threat that cyber capabilities pose to States and the private sector alike has rapidly increased. A 2024 threat report by CrowdStrike reflects a 60% global increase in the number of interactive intrusion campaigns by adversaries, with North America leading the surge.[16] The National Security Agency's 2023 cyber security report reflects similar trends, emphasizing a global landscape that is becoming more complex as technology advances.[17] The threat posed by cyber capabilities is no doubt becoming more common, more complex and more pervasive. In a word, cyber operations are now or will soon become ubiquitous in both everyday life as well as war.

Ongoing conflicts reinforce the point. Throughout the Ukraine–Russia conflict, both belligerents have used cyber capabilities to support and achieve

9 DoD, Joint Chiefs of Staff, *Capstone Concept for Joint Operations*, Joint Publication Ver. 2.0, August 2005, p. 7.

10 US Cyber Command, "Our History", available at: www.cybercom.mil/About/History.

11 *Ibid.* A unified combatant command is a military command that has a broad, continuing mission and is composed of forces from two or more military departments. 10 US Code § 161(c)(1). There are eleven unified combatant commands: seven with geographical areas of responsibility, and four with transregional responsibilities (Cyber Command, Special Operations Command, Strategic Command and Transportation Command). DoD, "Combatant Commands", available at: www.defense.gov/About/combatant-commands/.

12 NATO, "Warsaw Summit Communiqué", 9 July 2016, available at: www.nato.int/cps/en/natohq/official_texts_133169.htm.

13 NATO, "Prague Summit Declaration", 21 November 2002, available at: www.nato.int/cps/en/natohq/official_texts_19552.htm.

14 NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), "About Us", available at: https://ccdcoe.org/about-us.

15 Michael N. Schmitt, "Noteworthy Releases of International Cyber Law Positions – Part 1: NATO", *Articles of War*, 27 August 2020, available at: https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i.

16 Interactive intrusion techniques involve adversaries actively executing actions on a host to accomplish malicious objectives, unlike malware attacks, which depend on deployment of pre-established tools and scripts. CrowdStrike, *2024 Global Threat Report*, 2024, p. 10, available at: www.crowdstrike.com/global-threat-report/.

17 US National Security Agency, *2023 NSA Cybersecurity: Year in Review*, 2023, p. 3, available at: www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3621654/nsa-publishes-2023-cybersecurity-year-in-review/.

their operational goals.[18] The second invasion phase of that conflict began with a massive and successful cyber operation against Viasat, an American satellite company that provided internet connections to much of Ukraine, with Russia using destructive wiper malware to disable and destroy Viasat modems and routers.[19] The operation launched just hours before the 2022 physical invasion. Since then, Moscow has worked persistently to disrupt Elon Musk's Starlink transmissions in Ukraine through cyber and kinetic means.[20] Similarly, both Israel and Hamas appear to rely on the cyber domain for military advantage in their ongoing conflict. From cyber attacks on the Israeli government and security sectors to widespread Israeli communications blackouts in the Gaza Strip, it is clear that the use of the cyber domain to achieve military advantage is more or less guaranteed in the wars of today and those of the future.[21]

Cyber integration

Just as important as the fact of their wartime use is *how* armed forces will use cyber operations during armed conflict. Recently updated military doctrine confirms the merger and integration of a wide range of cyber operations into conventional military planning and concepts. Cyber operations are increasingly considered part of, rather than distinct from, the conventional capabilities that armed forces employ in war. US military doctrinal sources routinely refer to both "kinetic and non-kinetic … fires".[22] The former category includes conventional strikes relying on releases of stored energy for effects, while the latter describes "actions designed to produce effects without the direct use of the force or energy of moving objects and directed energy sources".[23] In practical terms, non-kinetic fires typically employ assets other than traditional weapons, including electromagnetic or cyber tools.[24]

18 Ukraine's IT Army executes daily cyber attacks against Russian services, from radio stations to food supply lines. Joe Tidy, "Meet the Hacker Armies on Ukraine's Cyber Front Line", *BBC News*, 14 April 2023, available at: www.bbc.com/news/technology-65250356; "Several Ukrainian State-Run Bodies Report Cyber Attacks", *Reuters*, 25 January 2024, available at: www.reuters.com/technology/cybersecurity/several-ukrainian-state-run-bodies-report-cyber-attacks-2024-01-25/.

19 Patrick Howell O'Neill, "Russia Hacked an American Satellite Company One Hour before the Ukraine Invasion", *MIT Technology Review*, 10 May 2022, available at: www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

20 Alex Horton, "Russia Tests Secretive Weapon to Target SpaceX's Starlink in Ukraine", *Washington Post*, 18 September 2023.

21 Tal Mimran, "Israel–Hamas 2023 Symposium – Cyberspace – the Hidden Aspect of the Conflict", *Articles of War*, 30 November 2023, available at: https://lieber.westpoint.edu/cyberspace-hidden-aspect-conflict.

22 DoD, *Summary of the Joint All-Domain Command and Control Strategy*, March 2022, p. 6, available at: https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/summary-of-the-joint-all-domain-command-and-control-strategy.pdf.

23 DoD, Joint Staff J7, *Integration and Synchronization of Joint Fires*, 4th ed., July 2018, p. 3, available at: www.jcs.mil/Portals/36/Documents/Doctrine/fp/int_and_sync_jointfires.pdf?ver=2018-09-18-102801-350.

24 *Ibid.*, p. GL-1; Major Carrie Salas, "Integrating Lethal and Nonlethal Effects", Air Land Sea Space Application Center, 15 August 2021, available at: www.alsa.mil/News/Article/2732245/integrating-lethal-and-nonlethal-effects.

New US military doctrine directs commanders to integrate both forms of fires, kinetic and non-kinetic, in all domains of war under the guise of multi-domain operations.[25] A senior US leader recently lamented past failure in that respect, observing that "for the longest time we kept different types of fires (example, strike, info ops, and cyber) separated and compartmented and did not fully realize their interdependencies".[26] Emerging doctrine on multi-domain operations seeks to remedy this defect. It demands complete and seamless integration of cyber capabilities and units into all combat operations.[27]

A 2023 US Army publication, vaguely titled *Information*, provides important details concerning the integration of cyber forces, tools and operations into warfighting.[28] It aligns the Army's approach to the larger information realm with the US vision for multi-domain operations. It also elevates information activities and considerations from their former status as supporting aspects of conflict to full warfighting functions in their own right.[29] The publication summarizes the approach and instructs Army commanders to more clearly account for information capabilities and effects as follows:

> Army forces employ information in combination with physical action to influence threat decision making and behavior. They attack threat data, information, and networks to influence threat perceptions and behavior and to affect the threat's ability to exercise command and control of its own forces.[30]

The directive to "attack" as an information activity is particularly eye-catching. It reflects an active, even aggressive mindset toward information activities. Among four principles to guide pursuit of information advantage, the publication directs that actions be "offensively oriented".[31] Offensive orientation envisions seizing and maintaining the initiative over enemy information activity, acting quickly against adversary information platforms and adapting rapidly to deprive enemy forces of potential information advantages.[32] At every turn, this new doctrine conditions commanders to think of information as part of, rather than as supporting, combat power – an integral part of the "total means of destructive and disruptive force that a military unit/formation can apply against an enemy".[33] It instructs Army forces to "employ all relevant capabilities to attack threat data, information, and networks".[34]

25 US Department of the Army, above note 7, p. 1-2, para. 1-9.
26 DoD, above note 23, p. i.
27 *Ibid.*, p. 10.
28 US Department of the Army, *Information*, Army Doctrine Publication 3-13, 27 November 2023.
29 *Ibid.*, p. 2-6. As an interesting aside, the US Army and DoD have abandoned the term "information operations". Personal connections indicate that pejorative political and censorship connotations are behind the shift.
30 *Ibid.*, p. vii.
31 *Ibid.*, p. ix.
32 *Ibid.*, p. 2-14, paras 2-62–2-63.
33 *Ibid.*, p. 1-5, para. 1-17.
34 *Ibid.*, p. 1-6., para. 1-19.

A DoD-level publication offers a similarly broad and vigorous attitude toward information power. It characterizes information power as "the ability to exert one's will through the projection, exploitation, denial, and preservation of information".[35] In a surprisingly frank though no doubt accurate assessment, the aforementioned *Information* document identifies "smartphones, the internet, and social media" as information platforms relevant to warfighting.[36] Both sources anticipate the same approach to information by US adversaries;[37] commanders are advised to anticipate that enemy "information warfare" attacks will target "data and information, telecommunications systems and infrastructure, population groups, and relevant actors".[38]

Other elaborations on the *Information* attack directive are worth attention for later legal consideration. First, extensive US and adversary reliance on cyberspace and electromagnetic spectrum (EMS)-reliant technologies explain the publication's emphasis on developing information attack capabilities.[39] Few States seem capable of fighting to their full potential in a cyber-degraded battlespace. Denying, disrupting, destroying or manipulating a broad range of the enemy's cyber and EMS systems (including, as noted above, "smartphones, the internet, and social media"), as well as the data they store and transmit, are attack priorities. Anticipated military advantages of these attacks include degrading adversary command and control and reducing an enemy's own information warfare capabilities.[40]

Second, like generally applicable US targeting doctrine, information attack doctrine emphasizes effects over destruction for its own sake. In conjunction with kinetic targeting means, combinations of "electromagnetic attack, cyberspace attack … [and] classified capabilities" are intended to achieve adverse effects on an enemy's ability and will to resist.[41] Destruction, degradation or denial of a target system or data are of far less significance than the impact these actions have on enemy operations and the tactical, operational or strategic advantage they create. Targets may be selected not according to their nature but rather according to how the enemy uses or may use them. Beyond obvious enemy military assets, information attack doctrine identifies "cyberspace reconnaissance, social media exploitation, and collection of publicly available information" as important sources of adversary military advantage, the deprival or disruption of which produces significant military effects.[42]

Finally, and importantly for the purposes of later discussion of international legal considerations, information doctrine uses the term "attack" broadly. Beyond the effect of destruction, US military thinking understands less

35 DoD, *Information in Joint Operations*, Joint Publication 3-04, 14 September 2022, p. ix.
36 US Department of the Army, above note 28, p. 1-6, para. 1-21.
37 *Ibid.*, pp. 1-7, 1-12–1-13, paras 1-42–1-48; DoD, above note 35, pp. I-3–I-4, IV-5.
38 US Department of the Army, above note 28, p. 1-14, para. 1-48.
39 *Ibid.*, p. 7-1, para. 7-1.
40 *Ibid.*, p. 7-1, para. 7-3.
41 *Ibid.*, p. 7-2, para. 7-4.
42 *Ibid.*, p. 7-5, para. 7-28.

severe effects such as disruption, degradation and manipulation as important attack effects.[43] Operations that produce immediate effects short of physical destruction, including jamming, manipulating content, slowing function or blocking access to adversary information assets, against a broad array of targets, are widely included in the ambit of information attack in US operational doctrine.

Dispersion

The maturation of the cyber domain as a full-fledged and integrated warfighting realm coincides with a revolution in US concepts of wartime command and control. The scale, pace and lethality of future large-scale combat operations are thought to require significant adjustments to the facilities and procedures that direct and supervise fighting units. Survival in an environment of omnipresent sensors and accurate long-range fires will require wide geographic dispersal of forces and headquarters. Military theorists assert that this form of fighting will demand an operational area so large that States' armed forces cannot form for linear, continuous attacks; instead, effective operations will require the physical separation of forces and their headquarters in order to operate independently in smaller, cellular elements.[44]

This non-linear, dispersed character of future warfare will greatly complicate communications and coordination between units and their respective headquarters.[45] Long-standing US doctrine has expected command and control systems to function in the setting of integrated and consolidated command posts.[46] Successful and effective command posts have been physically configured into large, consolidated facilities to ensure the efficient passage of information from one staff element to another. Newly updated doctrine, however, emphasizes command post scattering and mobility to avoid attack. The massive, centralized command posts seen in recent counter-insurgency and counterterrorism campaigns will not be tenable or able to survive in large-scale combat operations, owing in large part to the large electronic signatures they emit.[47] New doctrine emphasizes that the size of a command post directly affects its electronic signature, and acknowledges that large command posts present great physical and

43 *Ibid.*, p. 7-6, para. 7-29.

44 James K. Greer, "LSCO Lessons: What the Army Should Be Learning about Large-Scale Combat Operations from the Ukraine War", Modern War Institute at West Point, 24 June 2022, available at: https://mwi.westpoint.edu/lsco-lessons-what-the-army-should-be-learning-about-large-scale-combat-operations-from-the-ukraine-war.

45 Sydney Feedberg, "Army Races to Adapt to New Command Post Threats", *Breaking Defense*, 7 August 2023, available at: www.realcleardefense.com/2023/08/07/army_races_to_adapt_to_new_command_post_threats_971174.html.

46 The aspects of a command and control system are people, processes, networks and command posts. US Department of the Army, *Commander and Staff Organization and Operations*, Field Manual 6-0, May 2022, p. 8-1.

47 Milford "Beags" Beagle, Jason C. Slider and Matthew R. Arrol, "The Graveyard of Command Posts: What Chornobaivka Should Teach Us about Command and Control in Large-Scale Combat Operations", *Military Review Online*, March 2023, available at: www.armyupress.army.mil/journals/military-review/online-exclusive/2023-ole/the-graveyard-of-command-posts.

electromagnetic risk.[48] Physical dispersion to minimize electronic and other communications emissions is therefore required. And like their colleagues in the intelligence, operations and logistics staff sections, military legal practitioners and their commanders must prepare to function in a fractured version of command and control, facing communication challenges at a scale not seen in recent armed conflict.

Delegation

Distinct from – though related to – command dispersal is the notion of delegation. It is not widely appreciated that US military lawyers spend enormous amounts of time and energy analyzing and advising on sources of domestic operational and legal authority to conduct operations. Every command function and activity must be clearly grounded in an express source of command authority.[49] As noted above with respect to dispersion, emerging US command doctrine envisions planning, decision-making and fighting in significantly dispersed and even degraded environments, particularly with respect to information systems.[50] To rely on unified or national-level organizations to command forces and direct warfighting in this environment courts delay and disaster. Disruptions of communications will likely require delegations of both operational and legal authority to act quickly and decisively, including in the cyber domain.

For now, it appears that most States restrict authority to approve many cyber operations, particularly offensive cyber operations, to their highest levels of government.[51] For example, publicly available sources identify US approval authority for offensive cyber operations at the presidential level, unless specific operations are delegated to the secretary of defence.[52] Even recently updated US information doctrine does not clearly or publicly anticipate independent cyber operations authority at the brigade (approximately 3,000–5,000 soldiers) or lower levels.[53] To that end, commanders and their staffs are cautioned that coordinating for space and cyberspace capabilities often requires coordination and approval through the headquarters of several Army echelons.

48 US Department of the Army, above note 46, p. 8-9.

49 US joint doctrine places responsibility on legal advisers to identify relevant legal authorities (including law, policies, treaties and agreements) in mission analysis. Military lawyers are charged with providing this information to commanders and planners to shape military planning. DoD, *Legal Support to Military Operations*, Joint Publication 1-04, 2 August 2016, pp. II-7, II-8.

50 US Department of the Army, above note 28, p. vii.

51 Suzanne Smalley, "Biden Administration Is Studying Whether to Scale Back Trump-Era Cyber Authorities at DOD", *Cyberscoop*, 31 March 2022, available at: https://cyberscoop.com/biden-trump-nspm-13-presidential-memo-cyber-command-white-house/; Michael P. Carvelli, "A Smarter Approach to Cyber Attack Authorities", *Joint Forces Quarterly*, Vol. 91, 2018, available at: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-91/jfq-91_67-73_Carvelli.pdf?ver=2018-11-05-155114-413.

52 Paul C. Ney Jr, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference", 2 March 2020, available at: www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

53 US Department of the Army, above note 28, p. 7-2, para. 7-7.

Though they represent an understandably cautious approach considering the sensitive, interconnected and overwhelmingly civilian nature of cyberspace, these processes are often cumbersome and inefficient. While policies requiring high-level approval for cyber activity may be appropriate outside the context of armed conflict, the intensity and pace of modern warfare, particularly large-scale combat operations, seems likely to demand delegation to lower levels of command. Current authority structures are particularly at odds with the integration and synchronizations of kinetic and non-kinetic fires envisioned in emerging US multi-domain warfighting doctrine.

There are, however, signs that such adjustments to wartime cyber authorities may already be under way.[54] US targeting doctrine already instructs commanders to "gain authorities and permissions for Information Related Capabilities to broaden options", and to "[b]e prepared to spend time gaining authorities and permissions for info-related capabilities".[55] And the procedural vehicles for requesting such authorities are in place and well practiced by military lawyers – for example, US standing rules of engagement provide familiar and ready-made procedures for such delegations.[56]

While responsive to the emerging demands of large-scale combat and multi-domain operations, in a legal sense, delegations of authority require that lower levels of command understand the application of international law to a broader operational range and in greater depth than previously. Together, the growth of States' military cyber forces, clear doctrinal signals that cyber operations will be integral to warfighting, and greater delegation of authority to conduct cyber activities make a compelling case for renewed attention to how the law of armed conflict regulates cyber means and methods of war as well as the extent to which supporting legal doctrine is fit for that purpose.

US wartime cyber law doctrine

Early legal assessments of cyber military operations devoted significant attention to determining whether the law of war applied at all to the cyber realm.[57] The novelty and idiosyncrasies of the cyber domain, the historical settings of law of war formation, and political considerations had led some to resist the application of the law of war to activities in cyberspace.[58] However, the prevailing view, including that of the United States, now clearly holds that cyber means are fully

54 M. P. Carvelli, above note 51.
55 DoD, above note 23, pp. 1–2.
56 US Chairman of the Joint Chiefs of Staff, "Standing Rules of Engagement/Standing Rules for the Use of Force", Instruction 3121.01B, 13 June 2005.
57 Michael N. Schmitt, "Wired Warfare: Computer Network Attack and *Jus in Bello*", *International Review of the Red Cross*, Vol. 84, No. 846, 2002, pp. 365, 368–375.
58 See e.g. Adam Segal, "China, International Law and Cyber Space", Council on Foreign Relations, 2 October 2012, available at: http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace/.

capable of activating the law of war's "armed conflict" threshold and that its rules and principles regulate wartime resorts to cyber capabilities.[59]

Attention – military, humanitarian and academic – has shifted to questions relating to *how* the law of war applies to cyber operations. Views are available from a range of sources and can be distinguished in large part according to the degree of determinacy they provide. For US military lawyers, the DoD *Law of War Manual* (DoD Manual) is the most comprehensive and influential source of law of war doctrine.[60] Its stated purpose is "to provide information on the law of war to DoD personnel"[61] – yet few if any US military lawyers can claim comprehensive familiarity with the DoD Manual. Its size and density prevent most judge advocates from full, rote knowledge of its guidance; instead, it serves (and was likely intended) as a work of reference to be consulted rather than internalized.

Despite its size and purpose, the DoD Manual leaves much unexplained.[62] For instance, because the United States has signed but not ratified Additional Protocols I and II to the 1949 Geneva Conventions, the legal basis for many rules applicable to the conduct of hostilities is not always entirely clear. Moreover, although the DoD Manual often expresses rules in language identical or similar to Additional Protocols I and II, it does not always indicate whether many of their provisions reflect customary international law.[63] The Manual also confines itself almost exclusively to rules derived from the law of war, a position that is not surprising in light of long-standing restrictive US legal policies concerning the applicability of other legal regimes, such as international human rights law, to armed conflict.[64]

Prominent among the DoD Manual's chapters addressing specialized realms of warfighting – including those on the sea, in space and in the air – is its cyber operations chapter.[65] This chapter materialized shortly after US recognition of cyberspace as an operational domain,[66] yet, even at the date of its publication, it was clear that the Manual had left pressing questions concerning international

59 Referring to the applicability of international humanitarian law to cyberspace in conflict, see *Report of the Group of Governmental Experts on Advancing Responsible Behavior in Cyberspace in the Context of International Security*, UN Doc. A/76/135, 14 July 2021, p. 18. Reflecting the overwhelming national positions that international humanitarian law applies in cyberspace, see "International Humanitarian Law (Jus in Bello)", *Cyber Law Toolkit*, available at: https://cyberlaw.ccdcoe.org/wiki/International_humanitarian_law_(jus_in_bello); Caroline Krass, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference", 18 April 2023, available at: www.defense.gov/News/Releases/Release/Article/3369498/dod-general-counsel-delivers-keynote-remarks-at-us-cyber-command-legal-conferen/.

60 DoD, Office of the General Counsel, *Law of War Manual*, June 2015, updated July 2023 (DoD Manual).

61 *Ibid.*, § 1.1.1.

62 In its current edition, the DoD Manual runs to well over 1,200 pages and nearly 7,100 footnotes. At fifteen pages and seventy-eight footnotes, the "Cyber Operations" chapter is by far the shortest and most lightly sourced in the Manual. *Ibid.*, pp. 1024–1039.

63 William H. Boothby and Wolff Heintschel von Heinegg, *The Law of War: A Detailed Assessment of the US Department of Defense Law of War Manual*, Cambridge University Press, Cambridge, 2018, p. 7.

64 Michael J. Dennis, "Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation", *American Journal of International Law*, Vol. 99, No. 1, 2005.

65 DoD Manual, above note 60, pp. 1024–1081.

66 DoD, *Cyberspace Operations*, Joint Publication 3-12, 5 February 2013, p. GL-4; DoD, *Joint Operations*, Joint Publication 3-0, 11 August 2011.

law and cyber operations unaddressed.[67] Likely owing to the still-nascent condition of State cyber practice, the DoD Manual declined to stake out meaningful positions on a number of cyber-related legal issues. And although DoD has updated and reissued the Manual three times since 2015, it has made no substantive changes to the cyber operations chapter.[68]

The DoD Manual often declines to offer the doctrinal detail or precision found in other legal resources. Modern judicial decisions, humanitarian organizations' publications and academic law of war scholarship often greatly exceed the Manual in terms of detail and interpretation.[69] By comparison with these sources, the Manual frequently preserves a high degree of legal indeterminacy. That observation is particularly true of the Manual's cyber chapter, which observes that

> [p]recisely how the law of war applies to cyber operations is not well-settled, and aspects of the law in this area are likely to continue to develop, especially as new cyber capabilities are developed and States determine their views in response to such developments.[70]

The law of war attack threshold

Prominent among these "how" questions is the translation of the important law of war notion of "attack" to the cyber context. The law of war now offers a highly refined regulatory regime for operations that amount to attack. While it is tempting to apply these rules outside the context of attack, doing so as a matter of law risks profound legal error. Indeed, no step toward identifying the correct legal framework for a wartime cyber operations may be more important than the attack/non-attack determination.

At its outset, the DoD Manual's cyber chapter helpfully reminds readers that operations colloquially termed "cyber attacks" are not necessarily attacks for law of war purposes. Casual resort to the term "cyber attack" as a generic reference to any manner of malicious activity or event in cyberspace abounds in news media and even in technical and doctrinal publications. Thus, the Manual offers several examples of malicious though sub-attack cyber operations, including "defacement of websites, network intrusions, the theft of private

67 Sean Watts, "Cyber Law Development and the United States Law of War Manual", in Anna-Maria Osula and Henry Rõigas (eds), *International Cyber Norms: Legal Policy and Industry Perspectives*, NATO CCDCOE, Tallinn, 2016.

68 After initial publication in June 2015, the DoD Office of General Counsel promulgated updates and reissued the DoD Manual on 31 May 2016, 13 December 2016 and 31 July 2023. DoD Manual, above note 60, pp. 1207 ff.; Emily E. Bobenrieth, "2023 DoD Manual Revision – What Was Left Unsaid for Cyber Operations", *Articles of War*, 14 September 2023, available at: https://lieber.westpoint.edu/what-was-left-unsaid-cyber-operations/.

69 As but one example, both courts and academia have written at extraordinary length on the law of war question of conflict classification: see e.g. Elizabeth Wilmshurst (ed.), *International Law and the Classification of Conflicts*, Oxford University Press, Oxford, 2012. By comparison, guidance in States' military legal manuals on the subject is scant, even anaemic.

70 DoD Manual, above note 60, § 16.1.

information, or the disruption of … internet services".[71] Cataloguing other examples of military cyber operations that may not amount to attacks under the law of war, the Manual offers

> reconnaissance (e.g., mapping a network), seizure of supporting positions (e.g., securing access to key network systems or nodes), and pre-emplacement of capabilities or weapons (e.g., implanting cyber access tools or malicious code). In addition, cyber operations may be a method of acquiring foreign intelligence unrelated to specific military objectives, such as understanding technological developments or gaining information about an adversary's military capabilities and intent.[72]

These examples make the important operational point that non-attack cyber activities are essential and expected facets of modern warfighting. They also illustrate that a wide range of cyber activities during warfare may be conducted free from the legal restraints applicable to *de jure* attacks.

To that end, the DoD Manual's cyber chapter repeatedly emphasizes the attack threshold as a critical step in legal analysis of cyber operations. It first instructs that cyber operations amounting to attack must comply with law of war targeting rules, including those of distinction and proportionality.[73] The chapter indicates that a cyber attack which destroys enemy computer systems would be unlawful if directed against civilian objects, including cyber infrastructure.[74] In its simplest expression, the rule of distinction requires that belligerents only direct attacks at combatants and persons taking direct part in hostilities,[75] and that they not attack other persons. With respect to objects, the rule requires belligerents to limit attacks to military objectives, and to spare civilian objects. It is perhaps the most important rule of the law of war, an assessment reinforced by the Additional Protocol I (AP I) article that codifies the rule for that instrument's States Parties, entitled "Basic Rule".[76]

While indeed fundamental, the obligation to distinguish combatants from civilians and military objectives from civilian objects does not apply to all wartime conduct. Any number of presumably non-attack military activities may be lawfully directed at either civilians or civilian objects during war. These include, to name only a few, intelligence collection, internment, search, requisition, confiscation, psychological operations, and electronic and other communication jamming.

71 *Ibid.*, p. 1026, § 16.1.3.2.
72 *Ibid.*, pp. 1025–1026, § 16.1.2.1.
73 *Ibid.*, pp. 1033–1034, § 16.5.1.
74 *Ibid.*, p. 1033, § 16.5.1.
75 *Ibid.*, p. 213, paras 5.5.1–5.5.2; Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, 8 June 1977 (entered into force 7 December 1978) (AP I), Art. 48.
76 Unlike those of the 1949 Geneva Conventions, which were added by the Swiss Federal Council after adoption, the article titles of AP I were included in its adopted form. AP I, Art. 48, in *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Geneva (1974-1977)*, Vol. 1, Federal Political Department, Bern, 1978, pp. 119, 146.

Yet curiously, the DoD Manual's cyber chapter offers no cyber-specific criteria for distinguishing attack from non-attack operations. It instead provides a cross-reference to the Manual's general discussion of the law of war attack threshold. And although that section addresses attack terminology, including phrases such as "object of attack", "direct attack" and "intentional attack", it offers no clarification on the term "attack" itself.[77]

While the cyber chapter lacks cyber-specific, positive criteria for assessing whether cyber activity amounts to attack, to its credit, a negative definition of sorts can be discerned from the chapter. A section addressing non-attack cyber operations concludes that operations resulting only in reversible or temporary effects do not amount to attacks. It further identifies defacements, disruptions of service, interference with communication, and propaganda as non-attack cyber operations. Importantly, the section indicates that such operations, and presumably any other non-attack cyber activity, "need not be directed at military objects, and may be directed at civilians or civilian objects".[78] It immediately adds, however, that such operations "must not be directed against enemy civilians or civilian objects unless the operations are militarily necessary".[79]

Recent academic literature on the attack threshold in cyber contexts reveals that the DoD Manual's cyber chapter has left much unaddressed. For instance, in its chapter on conduct of hostilities, the *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* (Tallinn Manual 2.0) offers extensive analysis of law of war attack rules.[80] Although not a NATO- or State-endorsed product, the Tallinn Manual 2.0 has been highly influential. Many views offered in it, including minority views of the group that drafted it, have found expression in subsequent State expression on international law and cyber operations.[81]

The Tallinn Manual 2.0 addresses in detail cyber attacks against persons and against objects, and precautionary rules applicable to attack. Concerning the notion of "attack" itself, it recites Article 49(1) of AP I, emphasizing especially the element of violence. According to the Tallinn Manual, violence extends beyond the release of kinetic force to include means involving and effects resulting from cyber operations. The Manual maintains that violence resulting from a cyber operation in the form of death, injury, destruction or damage is sufficient to amount to an attack.[82]

However, the Tallinn Manual 2.0's group of experts was split on important questions relating to the attack threshold. For instance, the group agreed that

77 DoD Manual, above note 60, p. 198, § 5.4.1.
78 *Ibid.*, p. 1035, § 16.5.2.
79 *Ibid.*, p. 1035, § 16.5.2.
80 In 2013, at the invitation of the NATO CCDCOE, a group of experts published the first Tallinn Manual: Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge 2013. The group updated and expanded the Manual in 2017: Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017 (Tallinn Manual 2.0).
81 Reflecting State positions that international humanitarian law applies in cyberspace, see "International Humanitarian Law (Jus in Bello)", above note 59.
82 Tallinn Manual 2.0, above note 80, pp. 415–416, Rule 92, paras 4–6.

operations against data which in turn foreseeably produce physically destructive effects qualify as attacks.[83] Still, whether cyber operations that confine destruction or damage to data, *as such*, amount to attacks produced a range of opinions. A majority concluded that they do not because data are "intangible" and do not fall within the plain meaning of the term "object".[84] The question of whether cyber operations that merely affect functionality of target systems amount to attacks also produced a variety of opinions, with a minority of the experts concluding that they do not.[85] And while the majority of experts concluded that effects on functionality may satisfy the violence element of the attack threshold, that majority was split on more specific questions relating to the nature and degree of function loss and the remedial measures required to restore functioning.[86] Meanwhile, a growing body of academic and humanitarian scholarship has similarly staked out a wide range of views, many quite expansive, on cyber operations and the law of war attack threshold.[87]

Likely prompted by these private writings, as well as by mounting operational experience, many States, including US allies, have offered refined views on cyber operations and the attack threshold.[88] For example, Israel recently expressed the view that only cyber operations resulting in physical damage meet the violence element of the law of war attack threshold.[89] France, by contrast, offers a broad interpretation of cyber operations amounting to attack. Its Ministry of Armies' recent statement on international law and cyberspace maintains that if targets "no longer provide the service for which they were implemented, whether temporarily or permanently, reversible or not", the cyber operation that produced these effects amounts to an attack.[90] For its part, Australia has offered an ambiguous position, simply instructing its forces that cyber activity may amount to attack if "it rises to the same threshold as a kinetic 'attack'". That view has prompted some to presume that effects on functionality or that require repair

83 *Ibid.*, p. 416, Rule 92, para. 6.
84 *Ibid.*, p. 437, Rule 100, para. 6. A minority of the group concluded that certain data can be regarded as an object: *ibid.*, p. 437, para. 7.
85 *Ibid.*, p. 417, para. 10.
86 *Ibid.*, pp. 417–418, Rule 92, paras 10–13.
87 See e.g. Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, "Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts", *International Review of the Red Cross*, Vol. 102, No. 913, 2020; International Committee of the Red Cross (ICRC), "Executive Summary: Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts", *International Review of the Red Cross*, Vol. 104, No. 919, 2022; ICRC, "International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper Submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019", *International Review of the Red Cross*, Vol. 102, No. 913, 2020.
88 See e.g. Michael N. Schmitt, "Big Data: International Legal Issues in Armed Conflict", in Laura A. Dickinson and Edward W. Berg (eds), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold*, Lieber Studies, Vol. 9, Oxford University Press, Oxford, 2024, pp. 151, 156-158.
89 Roy Schörndorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies*, Vol. 97, 2021, pp. 395, 404.
90 French Ministry of the Armies, "International Law Applied to Operations in Cyberspace", 2019, p. 13.

notwithstanding lack of physical damage amount to attack under the Australian view;[91] a contrary conclusion, however, cannot be ruled out.

A slew of other law of war rules accompanies and supports the rule of distinction. Like the rule itself, however, each is usually understood only to apply to operations amounting to attack. A particularly important though problematic rule is the obligation to take feasible precautions.[92] The DoD Manual's cyber chapter offers unclear advice concerning this duty; precautions are a ruleset usually associated with the law of war attack regime, but the cyber chapter may suggest to some readers that precautions apply to "cyber operations" rather than only to cyber attacks. Two readings of the relevant section are possible.

By the first and perhaps plainest reading, the chapter's choice of the term "cyber operations" rather than "attacks" is understood to be deliberate and to indicate that all cyber operations, including those that do not amount to attack, require law of war precautions. As noted previously, US cyber operational doctrine views influencing the entirety of the information sphere as relevant to multi-domain operations. Such wartime cyber operations could foreseeably affect and even harm civilians and civilian objects. The urge to recognize a legal duty to take precautions to mitigate harmful effects on civilians during such operations, including an obligation to minimize incidental cyber effects, is understandable.

By the second reading, however, the DoD Manual's cyber chapter could be understood to indicate that all cyber operations merely require *consideration* as to whether precautions apply as determined by the chapter's preceding guidance on the attack threshold. This latter reading is preferred. It is consistent with the chapter's preceding insistence that attack rules only apply to operations amounting to attack, and it also better aligns with the chapter's succeeding two examples of precautions in a cyber context, both of which refer to "attack".[93] The narrow reading also tracks well with that section's instruction that precautions "should", as opposed to "must", be applied to cyber operations.[94] Additionally, the DoD Manual's general chapter on conduct of hostilities applies the term "must" with respect to precautions in attack and the term "should" with respect to precautions in kinetic non-attack activities of destroying or seizing enemy property already under one's control.[95] Finally, this narrow reading comports well with the October 2014 US statement to the United Nations Group of Governmental Experts indicating that the precaution of reducing incidental effects applies to death, injury and damage to civilians and civilian objects, effects usually indicative of an attack.[96] All the same, it would be helpful if the DoD

91 M. N. Schmitt, above note 88, p. 157.
92 See Sean Watts, "Law-of-War Precautions: A Cautionary Note", in Ronald T. P. Alcala and Eric Talbot Jensen (eds), *The Impact of Emerging Technologies on the Law of Armed Conflict*, Lieber Studies, Vol. 2, Oxford University Press, Oxford, 2019, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3202852.
93 DoD Manual, above note 60, p. 1036, § 16.5.3.
94 *Ibid.*, p. 1036, § 16.5.3.
95 *Ibid.*, p. 191, § 5.2.3.
96 "United States Submission", above note 1, p. 737.

Manual's cyber chapter were to include a clearer expression and cyber-specific comment on precautions with respect to non-attack activities.

The non-attack legal framework

In armed conflict, the number and nature of rules applicable to attack operations differs significantly from operations below that threshold, as does States' doctrinal legal guidance. To its credit, the DoD Manual's cyber chapter makes clear that law of war rules applicable to non-forcible means or methods of hostilities regulate non-attack cyber operations. The chapter cites and cross-references the Manual's general sections addressing destruction and seizure of enemy property in this regard.[97] However, the extent to which cyber operations can be analogized to such conventional wartime acts effectively and consistently by military lawyers is cause for concern. The cyber chapter acknowledges as much when it observes that

> [c]ertain cyber operations may not have a clear kinetic parallel in terms of their capabilities and the effects they create. Such operations may have implications that are quite different from those presented by attacks using traditional weapons, and those different implications may well yield different conclusions.[98]

Destruction and seizure

Destruction and seizure of enemy property, as well as requisition and confiscation during belligerent occupation, implicate succinct, almost cursory law of war rules. The Hague Regulations of 1907 simply state that the destruction or seizure of enemy property is forbidden unless doing so is required by imperative military necessity.[99] Other law of war instruments address destruction and seizure in similarly svelte provisions. Destruction or seizure may amount to a war crime or grave breach of the 1949 Geneva Conventions when "not justified by military necessity and carried out unlawfully and wantonly", and when undertaken against property protected under one of the four Conventions.[100] The Rome Statute of the International Criminal Court similarly prohibits "[d]estroying or seizing the enemy's property unless such destruction or seizure be imperatively demanded by the necessities of war".[101]

97 DoD Manual, above note 60, p. 1027, § 16.2.1, notes 10 and 12.
98 *Ibid.*, p. 1028, § 16.2.2.
99 Hague Convention (IV) respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land, 1907, Art. 23(g).
100 Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949, 75 UNTS 31 (entered into force 21 October 1950), Art. 50; Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of 12 August 1949, 75 UNTS 85 (entered into force 21 October 1950), Art. 51; Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War of 12 August 1949, 75 UNTS 287 (entered into force 21 October 1950), Art. 147.
101 Rome Statute of the International Criminal Court, 17 July 1998 (entered into force 1 July 2002), Art. 8(2)(b)(xiii); DoD Manual, above note 60, p. 1033, § 16.5.1.

Despite its earlier reference to destruction and seizure as relevant to non-attack cyber operations, the DoD Manual's cyber chapter offers no cyber-specific guidance on either of the above-mentioned rules of the Hague and Geneva Conventions. Instead, it cross references the Manual's general chapter on conduct of hostilities.[102] That section offers select elaborations on the rules of seizure and destruction. First, it re-emphasizes that both seizure and destruction must be "imperatively demanded by the necessities of war".[103] The imperative necessity standard is usually distinguished from that of mere necessity. The Manual earlier clarifies that law of war references to imperative or absolute military necessity, versus mere military necessity, "must not be conflated with mere convenience", suggesting an elevated or heightened standard for the former.[104] Imperative demand may be understood to require that no other option is available to achieve the same or similar military advantage.[105]

Importantly, the section leaves unaddressed the question of what acts constitute either destruction or seizure. This omission is perhaps understandable in the physical realm for which the section was written, where each act is relatively easily discerned with respect to physical objects and property. However, the question of whether many of the cyber acts that emerging doctrine counsels commanders to direct at adversary information capacity – including disruption, degrading, manipulation, rerouting and interception of communications and data – amount to destruction or seizure is unaddressed by either the general conduct of hostilities chapter or the cyber chapter, and therefore remains unclear.

Destruction, as a law of war term of art, is distinct from violence associated with attack, notwithstanding that the effects or consequences of destruction and attack may in fact be otherwise indistinguishable.[106] In fact, control of property is a critical concept in destruction – it is what distinguishes the violence prerequisite of attack from the violence inherent in destruction. The violence associated with the former is intended to deprive an adversary of control over an object or location,[107] whereas violence associated with the latter is usually understood to take place out of contact with the enemy and only against objects under a force's

102 DoD Manual, above note 60, p. 1027, § 16.2.1.

103 *Ibid.*, p. 294, § 5.17.

104 *Ibid.*, p. 55, § 2.2.2.2.

105 Sean Watts and Winston Williams, "Ukraine Symposium – Destructive Counter-Mobility Operations and the Law of War", *Articles of War*, 5 May 2022, available at: https://lieber.westpoint.edu/destructive-counter-mobility-operations-law-of-war.

106 Clearly distinguishing that the rules governing attacks are distinct from those that apply to destruction or seizure, see Chris Jenks, "Motive Matters: The Meaning of Attack under IHL and the Rome Statute", *Opinio Juris*, 26 October 2020, available at: https://opiniojuris.org/2020/10/26/motive-matters-the-meaning-of-attack-under-ihl-the-rome-statute/. Stating that "[o]utside the context of attacks, certain rules apply to the seizure and destruction of enemy property", see DoD, "Brief Overview of the Law of War for DoD Personnel", 6 August 2020, p. 6. Reflecting a "limited" right of destruction and generating criteria which must be met prior to engaging in destruction of enemy property, see Danish Ministry of Defence, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, 2020, p. 410, § 2.9.

107 Destroying an unoccupied dwelling for the purpose of depriving the enemy of a firing position in anticipation of future combat is one example of the destruction of enemy property distinct from an attack. Jeffrey A. Lovitky, "Rules Governing Property Destruction Outside of the Attack and

own control. The rules applicable to each activity are distinct and depend for their operation on an acute understanding of context. Similarly, physical control, usually to the exclusion of another, is the essence of seizure of property under the law of war.

As with so many concepts transposed from the physical to the cyber realm, however, defining and identifying cyber control can be complicated and thorny. Under what circumstances armed forces can be said to exercise control for purposes of distinguishing destruction from attack is particularly difficult to discern. Some cyber operations may undoubtedly give an armed force effective control over enemy infrastructure or data. That control may be highly analogous, for instance with respect to exclusion of enemy access or use, to the physical control that establishes conditions to which law of war destruction rules apply. Yet the DoD Manual's cyber chapter includes no cyber-specific guidance on control, either for purposes of law of war destruction analysis or otherwise.

The concept of seizure presents similar complications when applied to the cyber realm. It generally refers to the taking of a person or of property. As distinct from confiscation, seizure does not include a transfer of ownership rights.[108] Yet as noted previously, the DoD Manual offers examples of non-attack cyber activities involving "reversible or temporary effects" aimed at denying the enemy access to cyber infrastructure or data. Such operations could reasonably be equated to law of war seizures.[109] If so, denials of access to adversary digital property may be considered justified only by imperative military necessity.

For its part, the Tallinn Manual 2.0 confines treatment of seizure largely to settings of belligerent occupation.[110] Other sources, most notably the military legal manuals of important US allies, take a broader approach: some signal application of law of war rules governing seizure during the invasion phases of armed conflict.[111]

Finally, the DoD Manual's cyber chapter leaves unclear how exactly to conceive of the notion of property in reviews of wartime cyber operations.[112] Cyberspace is widely understood to be comprised of three interrelated layers: physical, logical and cyber-persona.[113] While defining property in the physical layer of cyberspace is not difficult (servers, wires, etc.), defining property in the logical layer can be complicated. The logical layer is inherently intangible, and workable, universally useful legal definitions are elusive.[114] While the instinct to

Occupation Contexts", *Articles of War*, 31 May 2024, available at: https://lieber.westpoint.edu/rules-governing-property-destruction-outside-attack-occupation-contexts/.

108 Danish Ministry of Defence, above note 106, p. 410, § 2.9.

109 DoD Manual, above note 60, p. 1035, § 16.5.2.

110 Tallinn Manual 2.0, above note 80, p. 544.

111 UK Ministry of Defence (MoD), *Joint Service Manual of the Law of Armed Conflict*, Joint Service Publication 383, 2004, para. 15.17; Danish Ministry of Defence, above note 106, p. 410.

112 DoD Manual, above note 60, p. 1033, § 16.5.1.

113 DoD, *Cyberspace Operations*, Joint Publication 3-12, 8 June 2018, p. I-3.

114 "Tangible Personal Property", in *Black's Law Dictionary*, available at: https://thelawdictionary.org/tangible-personal-property/. *Black's* defines tangible personal property as "touchable and moveable". That cyber property analogies may be ill-suited is apparent from efforts to adapt other legal regimes to the cyber context. Some efforts have abandoned notions of property ownership over objects in cyberspace in favour of rights of *access*. For example, patent law applies the concept of property to govern intangible resources – that is, the right to use an idea. Adam J. MacLeod, "Cyber Trespass and

analogize cyber phenomena, including aspects of the logical layer, to the physical world is understandable, clear evidence of States' intent to do so for legal purposes remains important, particularly for military legal advisers during armed conflict.

Constant care?

Lastly concerning putative non-attack rules, Article 57(1) of AP I states that "[i]n the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects".[115] A notoriously ambiguous provision, constant care has gained recent traction in law of war academic circles. In light of its generalized wording, some interpret its obligations as merely aspirational.[116] They argue that the constant care passage must be read in conjunction with the remainder of Article 57, comprised of rules that solely govern attacks.[117] That context, combined with the fact that the article title of Article 57 refers to "Precautions in Attack", leads proponents of this restrictive position to conclude that constant care only applies in the attack setting.[118]

However, a robust and growing body of private scholarship understands the constant care obligation more broadly. For example, the International Committee of the Red Cross (ICRC) considers that the use of the word "shall" indicates that this provision is binding on States party to AP I independently of the remainder of Article 57.[119] Moreover, the ICRC commentary to the article emphasizes that the words "military operations" in paragraph (1) should be understood to refer to "*any* movements, manoeuvres, and other activities whatsoever carried out by the armed forces with a view to combat".[120] The reference to "military operations" stands in contrast to the repeated "attack" references in paragraphs 2–5 of Article 57, indicating the former's application to "all domains of warfare and all levels of operations".[121]

Property Concepts", *IP Theory*, Vol. 10, 2021, p. 3, available at: https://iptheory.indiana.edu/cyber-trespass-and-property-concepts. In patent law, patent infringement is a form of trespass where a right of use is unlawfully violated: *ibid.*, p. 3. This body of law does not hinge on defining the property in question *per se*, but rather on defining how access and use are protected.

115 AP I, Art. 57(1).

116 Jean-Francois Quéguiner, "Precautions under the Law Governing the Conduct of Hostilities", *International Review of the Red Cross*, Vol. 88, No. 864, 2006, p. 793 (noting without adopting the aspirational view).

117 *Ibid.*, p. 796.

118 Chris Jenks and Rain Liivoja, "Machine Autonomy and the Constant Care Obligation", *Humanitarian Law and Policy Blog*, 11 December 2018, available at: https://blogs.icrc.org/law-and-policy/2018/12/11/machine-autonomy-constant-care-obligation/; Eliza Watt, "The Principle of Constant Care, Prolonged Drone Surveillance and the Right to Privacy of Non-Combatants in Armed Conflicts", in Russell Buchan and Asaf Lubin (eds), *The Rights to Privacy and Data Protection in Times of Armed Conflict*, NATO CCDCOE, Tallinn, 2022, p. 169.

119 International Law Association Study Group on the Conduct of Hostilities in the 21st Century (ILA Study Group), "The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare", *International Law Studies*, Vol. 93, 2017, p. 381.

120 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols*, ICRC, Geneva, 1987, p. 680. (emphasis added)

121 ILA Study Group, above note 119, p. 381.

Others in academia, including with respect to the cyber domain, also understand the rule of constant care as a "standalone" obligation.[122] The rule's expansive, continuous application to all military activities suggests to some that it should be extended beyond foreseeable physical harm and should apply to the protection from being subject to arbitrary interference with aspects of personal life and privacy.[123] Many States party to AP I directly support such an expansive view of constant care: for example, the United Kingdom considers "military operations", as the phrase appears in the constant care rule, to include even movements and deployments of armed forces.[124] The United Kingdom explains that "the commander will have to bear in mind the effect on the civilian population of what he is planning to do and take steps to reduce that effect as much as possible".[125]

For its part, the DoD Manual largely elides the notion of constant care. It includes no reference to constant care in its cyber chapter, and its general coverage of feasible precautions offers only a single concluding passage on constant care, framed in the third person with respect to AP I States Parties. The Manual simply notes: "Parties to AP I have agreed that '[i]n the conduct of military operations, constant care shall be taken ….' [They] may … interpret it in a manner consistent with the discussion in this section [on precautions]."[126]

In fairness, this summary treatment is in many respects justifiable. First, the United States, though a signatory State, is not a State party to AP I. Second, the DoD Manual seems to anticipate that much of what the constant care obligation amounts to is required by the feasible precautions obligation, covered in significant detail elsewhere in the Manual. Of course, that view does not account for the expansive understandings of constant care described previously. Third, many of the emerging and broad views of the constant care obligation, particularly concerning its cyber applications, post-date publication of the DoD Manual's cyber chapter. Last, it is likely that much of the protective work performed by the treaty-based constant care rule is understood by the United States to coincide with the broad regulatory functions that law of war principles perform. One of the present authors has previously commented elsewhere on the Manual's extensive treatment of law of war principles, including their binding character and role in regulating battlefield conduct.[127] Addressing cyber operations, the Manual advises that when no specific law of war rule applies, law of war principles guide conduct during wartime cyber operations.[128] All the same, an explicit and unequivocal evaluation as to whether the rule of constant care obligation reflects a customary

122 E. Watt, above note 118, p. 169.
123 *Ibid.*, p. 167.
124 MoD, above note 111, para. 5.32.
125 *Ibid.*, para. 5.32.1.
126 DoD Manual, above note 60, p. 196, § 5.2.3.5.
127 Sean Watts, "The DoD Law of War Manual's Return to Principles", *Just Security*, 30 June 2015, available at: www.justsecurity.org/24270/dod-law-war-manuals-return-principles.
128 DoD Manual, above note 60, p. 1026, § 16.2.

obligation in any form owed by US forces would be a constructive addition to the cyber chapter.

Concluding thoughts

On its initial publication, the cyber chapter of the DoD Manual was perhaps the right product for its time. It provided US military lawyers with an initial outline of international legal subjects relevant to emerging cyber operations, and it simultaneously accounted for the fledgling character of State cyber practice, particularly in war. The cyber chapter wisely reserved for later development many, if not most, interpretations of precisely how law of war rules operate with respect to wartime cyber activities.

Much has changed, however, since initial publication of the cyber chapter. Private manuals, scholarship and commentary have proffered greatly expanded analyses of concepts skimmed over by the chapter, including the law of war attack threshold, non-attack rules on destruction and seizure, and the putative constant care obligation. Instructing military lawyers to analogize to the physical contexts for which those rules were initially designed proved a useful start to adapting the law of war to cyberspace. However, it seems the broader law of war community, including many States, has matured beyond these analogies, advocating and adopting cyber-specific understandings of important law of war rules. Writings exist on the benefits and imperative of States contributing clear *opinio juris* to the greater law of war dialogue.[129] Those arguments apply with equal force to the operational cyber contexts described in this article, including command dispersion, delegation, and integrations of fires.

Debate concerning the attack threshold and applicability of attack-related rules to cyber operations is not merely academic – for instance, lack of consensus concerning operation of the attack definition in cyber operations prevented NATO from addressing the issue in a recent allied joint publication.[130] More important than keeping pace or competing with private and academic views, however, is ensuring that US military legal guidance keeps pace with the cyber operational picture. The cyber domain has matured greatly, both in technical and military doctrinal terms, since the initial publication of the cyber chapter. No longer a sideshow or supporting effort to warfighting, cyber operations and the cyber domain are becoming integral facets of the complex multi-domain sphere of war. The full integration of cyber operations into targeting processes ensures that such operations will be featured more regularly, against more objectives, and producing a wider range of effects than previously. Combined with the dispersion

129 Michael N. Schmitt and Sean Watts, "State *Opinio Juris* and International Humanitarian Law Pluralism", *International Law Studies*, Vol. 91, 2015, p. 171; Michael N. Schmitt and Sean Watts, "The Decline of International Law *Opinio Juris* and the Law of Cyber Warfare", *Texas International Law Journal*, Vol. 50, 2015, p. 189.

130 M. N. Schmitt, above note 15.

of forces and delegations of authority required by large-scale combat operations, the imperative to publish clear and up-to-date cyber legal doctrine is compelling.

It is easy, even for those indoctrinated to military dialect and culture, to discount large-scale combat operations, multi-domain operations and their accompanying concepts and doctrine, including integration, synchronization, command dispersal and delegation, as more Pentagon babble. But historically, the law of war has relied for its effectiveness on regular evolution and adaptation to changes in the character of war as expressed in military doctrine and practice in war. The emergence and maturation of cyberspace as a domain of warfare has in many ways outpaced law of war doctrine. States, including the United States, have shown little appetite for the sorts of deliberate and focused law-making efforts that have previously kept the law of war current and relevant. Meanwhile, much legal guidance that applies the existing law of war to wartime cyber operations rests on ambiguous platitudes and strained analogies that do not account for the operational realities of this most complex domain.

The mantra that "the law of war applies to all cyber operations" is no longer sufficient. This chant is void of the practical guidance that decision-makers require to confidently and legally manoeuvre in cyberspace. To remain on-pace with this domain and arm military advisers with the necessary legal tools, the United States must adapt law of war cyber doctrine to the realities of current and future warfare. Cyber will not wait; we must catch up.