CHAPMAN LAW REVIEW

Citation: Michael D. Minerva, *Through a Glass Darkly: Targeting Cyber and Space Infrastructure in the Law of War*, 29 CHAP. L. REV. 153 (2026).

--For copyright information, please contact chapman.law.review@gmail.com.

Through a Glass Darkly: Targeting Cyber and Space Infrastructure in the Law of War

Major Michael D. Minerva

CONTENTS

Through a Glass Darkly: Targeting Cyber and Space Infrastructure in the Law of War

*Major Michael D. Minerva**

As modern militaries become more capable in the cyber and space domains, much of the legal debate has focused on how to legally conduct cyber and space operations. While important, that discussion has largely overlooked the legal implications for the rapidly growing cyber and space infrastructure that exists in the physical domain—commercial satellites like Starlink filling the night skies and data centers like those popping up all over northern Virginia. Most of this infrastructure is commercially developed and privately owned—presumptively civilian in nature—and yet used by militaries all over the world.

The same way bridges form critical ground lines of communication subject to lawful attack under the Law of War, rapidly growing cyber and space infrastructure forms digital lines of communication that will become lawful military targets subject to attack. Kinetically targeting this infrastructure will have far-reaching distinction and proportionality implications that have largely been unaddressed despite perhaps being the simplest and most likely way states can affect the cyber and space domains. This Article takes a first step in assessing how the Law of War applies to this infrastructure and some of the targeting implications legal advisors and commanders must consider.

* Major Minerva is a judge advocate in the United States Marine Corps, presently assigned as the War Plans Officer at the United States Marine Corps Forces Central Command. He holds a Master of Operational Studies from the School of Advanced Warfighting, Marine Corps University, an LL.M. in National Security Law from the U.S. Army Judge Advocate General's School, a J.D. from Liberty University School of Law, and B.A.s in history and political science from Arizona State University. The opinions and conclusions expressed herein are solely those of the individual author and do not necessarily represent the positions of the Department of Defense, the Department of the Navy, or the United States Marine Corps.

I. INTRODUCTION: WE DREAMED THE FUTURE AND IT IS NOW

"For a few ecstatic moments Phaëthon felt himself the Lord of the Sky. But suddenly there was a change."[1]

The prospect of cyber and space war has loomed large in the American psyche for decades—whether it is Captain Kirk fighting tribbles, 007 fighting diamond-encrusted laser satellites, or John McClane protecting all of America's personal data. As the plots evolve into possibilities, the law struggles to keep up despite the decades of anticipation.

Not only are the plots of science fiction becoming realities, but capabilities are quickly outpacing our imaginations. Despite continuously evolving, the Law of War, like any body of law, struggles to address the evolving character of cyber and space warfare. Perhaps more than in other areas of the Law of War, the shroud of secrecy cast over cyber- and space-related technology makes discerning state practice and customary norms more difficult. Consequently, the literature on the topic tends to plod along at best, and to grope about in the dark at worst.

Despite prolific representation in films and television, actual space and cyber wars are even more common today than their media metaphors suggest. Unlike in film, however, at the center of space and cyber war is a commercially developed, privately owned infrastructure.[2] There is an ever-increasing military use of commercial satellites for access to cyber and space.[3] SpaceX's

---

1 EDITH HAMILTON, MYTHOLOGY 133 (12th prtg. 1959). Helios grants his mortal son, Phaëthon, one wish to prove his paternity. *Id.* at 132. Phaëthon, ignoring all wisdom and reason and not understanding the gravity of what he sought, chose to take his father's place for a day and drive the sun chariot through the sky. *Id.* at 132–33. "For a few ecstatic moments Phaëthon felt himself the Lord of the Sky," and then his feeble clutches at the reins alert the Sun's immortal horses that he has no control, so they run wild. *Id.* at 133. The chariot crashes into the constellations and then plunges to the earth below, setting the world on fire and turning rivers to steam. *Id.* Though repentant, Phaëthon perishes. *Id.* Greatly he dared, but, ignoring the customs and usages of the law, greatly he failed. *Id.*

2 *See, e.g.*, Julia Siegel, *Commercial Satellites Are on the Front Lines of War Today. Here's What This Means for the Future of Warfare.*, ATL. COUNCIL (Aug. 30, 2022), https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/commercial-satellites-are-on-the-front-lines-of-war-today-heres-what-this-means-for-the-future-of-warfare/ [https://perma.cc/EEA6-BFAS].

3 *See* Brandi Vincent & Mark Pomerleau, *Starlink Terminals Give Navy 'Game-Changing' Flexibility*, DEFENSESCOOP (Apr. 11, 2024), https://defensescoop.com/2024/04/11/starlink-terminals-navy-spacex-shipboard-c4i/ [https://perma.cc/AL9H-HY4D].

growing commercial satellite internet constellation has gained widespread military use—particularly as distributed operations, like those proposed in Expeditionary Advanced Base Operations (EABO), are implemented.[4] Commercial satellites are just one example of dual-use infrastructure relied on in cyber and space operations. Ultimately, any cyber operation that uses the internet as a method of gaining access or infiltrating a network makes that infrastructure dual-use.[5]

Cyberspace is often viewed as a public common akin to the ocean or the physical area of outer space (as distinguished from space infrastructure) or some sort of virtual reality matrix with no physical component. In reality, however, cyberspace is physically composed of networked computers and systems that are predominantly owned and operated by civilians.[6] This cyber infrastructure does far more than just provide internet for popular streaming platforms—markets and economies almost entirely rely on the existence of this infrastructure.[7] Moreover, operations in cyberspace inherently rely on this infrastructure. So, while it is comfortable to imagine cyber and space war as occurring in a galaxy far, far away, the truth is it is already streaming on a computer or server near you.

The existing literature tends to assess the Law of War implications of cyber and space operations as a world unto itself—separate from actual armed conflict—focusing singularly on how the Law

---

4 *See* Vincent & Pomerleau, *supra* note 3; Courtney Albon, *Reliant on Starlink, Army Eager for More SATCOM Constellation Options*, DEFENSENEWS (Aug. 21, 2024), https://www.defensenews.com/space/2024/08/21/reliant-on-starlink-army-eager-for-more-satcom-constellation-options/ [https://perma.cc/YJC3-7CUQ]; Paul Mozur & Adam Satariano, *Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service*, N.Y. TIMES (May 25, 2024), https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html [https://perma.cc/L3TW-R5ZM]; DEP'T OF THE NAVY, TENTATIVE MANUAL FOR EXPEDITIONARY ADVANCED BASE OPERATIONS 4-9 to -10 (2d ed. 2023).

5 Dual-use here refers to having a military and civilian use, vice nuclear and conventional use as in political science literature.

6 JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-12, CYBERSPACE OPERATIONS, at GL-4 (2018) (describing cyberspace as "[a] global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"); G. Alexander Crowther, *National Defense and the Cyber Domain*, THE HERITAGE FOUND. (Oct. 4, 2017), https://www.heritage.org/military-strength-topical-essays/2018-essays/national-defense-and-the-cyber-domain [https://perma.cc/4F7C-7E92].

7 See OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy* 17 (OECD, Working Paper No. 211, 2012).

of War applies to operations in cyberspace.[8] This Article will situate cyber operations within the context of armed conflict and flesh out the implications of the kinetic targeting of cyber and space infrastructure, exploring what happens when nominally civilian infrastructure becomes dual-use. Some questions this Article will address include: What does proportionality look like in that context? How much and what type of military use of a network is necessary in order for it to be a lawful military objective? Does attribution even matter if a country can identify and locate the cyber or space infrastructure used to attack it, and then kinetically destroy that infrastructure in self-defense regardless of where it physically resides?

These questions will become more and more prevalent as militaries continue to move toward contracted communications capabilities and support infrastructure. Unlike the historical Law of War developments relating to air and nuclear war, these questions must be addressed before the next major conflict—lest decision makers, like proud and youthful Phaëthon, lose control of capabilities they barely understand with consequences they refuse to foresee. This Article will explore these implications by using recent case studies as a starting point, but adding the additional facts necessary to contextualize them within the framework of armed conflict. Engaging in these hypotheticals will help develop a framework for decision making in response to cyber operations and normalize discussing kinetic responses to non-kinetic operations in the context of armed conflict.

To that end, Part II of this Article will describe the problem as it is today. Part III will present a possible cyber war scenario as a set of facts to analyze. Part IV will briefly survey fundamental principles of the Law of War and some specific implications in cyber and space war. Part V proposes a framework for analyzing the legal implications of targeting cyber and space infrastructure in *jus ad bellum* and *jus in bello* paradigms. Finally, Part VI applies that framework to the scenario developed in Part III. Ultimately, dual-use infrastructure—cyber, space, or otherwise—can

8 Gary Solis, and indeed most scholars, conceptually grant that a kinetic reprisal is a legitimate response to a cyber operation that constitutes a use of armed force. That, however, is as deep as most of the scholarship goes, without parsing out what cyber or space infrastructure becomes a military object. Much has been written about critical national infrastructure (e.g., power grids, transportation, finance, water supply systems, etc.) and its vulnerabilities, but again, the focus there has been on the lawfulness of cyber operations targeting critical national infrastructure, not the lawfulness of kinetically targeting cyber infrastructure. *See, e.g.*, GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 532–61 (3d ed. 2022).

be lawfully targeted, as long as the strikes provide a definite military advantage and reasonable precautions are taken to minimize collateral damage. Whether leaders are prepared to do so or the public is comfortable with that conclusion is another question entirely—that is why a sound targeting framework is critical.

II. THE FACTUAL AND LEGAL PROBLEMS OF DUAL-USE CYBER AND SPACE INFRASTRUCTURE

A. As a Matter of Fact

Cyber and space war receive a significant amount of written attention, both scholarly and journalistic. The more fact-intensive writing takes the form of investigative journalism, campaign analyses, or case studies, focusing on explaining what happened. Examples of these include *Countdown to Zero Day*,[9] *Dawn of the Code War*,[10] and *Dark Territory*.[11]

Of note, this body of literature often draws comparisons to other technological developments, primarily airplanes, nuclear weapons, and unmanned aerial vehicles (UAVs). While these comparisons are useful, they tend to fall short because those three technologies are more strictly military in nature, not dual-use, and, of even greater distinction, do not rely on civilian infrastructure as predominantly as cyber and space capabilities. The legal developments that those technologies drove (primarily about targeting dual-use objects) remain their chief utility for addressing cyber and space problems.

Finally, there is an almost myopic assumption throughout the literature that the only fathomable governmental responses to cyber operations fall into the diplomatic, informational, or economic parts of DIME,[12] with little thought given to what a traditional military response might entail.[13] Responses discussed tend

9 *See generally* KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON (2014) (exploring the Israeli-American cyber operation against Iranian enrichment facilities).

10 *See generally* JOHN P. CARLIN WITH GARRETT M. GRAFF, DAWN OF THE CODE WAR: AMERICA'S BATTLE AGAINST RUSSIA, CHINA, AND THE RISING GLOBAL CYBER THREAT (2018) (chronicling the Department of Justice's campaign against Chinese and Islamic State of Iraq (ISIL) cyber operations).

11 *See generally* FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR (2016) (outlining the history of cyber war).

12 JOINT CHIEFS OF STAFF, JOINT PUBLICATION 1, DOCTRINE FOR THE ARMED FORCES OF THE UNITED STATES, at I-12 to -13 (2017) (defining Diplomatic, Informational, Military, and Economic (DIME) as "instruments of national power").

13 As opposed to a military response that is a purely cyber operation response (tending to fall more in the informational category), vice a kinetic response. N.B.: No insinuation is intended that cyber operations are not "traditional . . . military activities" under 50

to include démarches, expulsion of diplomatic representatives, sanctions, criminal indictments and prosecutions, and punitive non-kinetic cyber operations. This tendency unfortunately has the side effect of narrowing discussion of the Law of War's applicability to cyber operations as explained below.

B. Legally Speaking

While there is a significant amount of literature arguing for policy change and legislation, many scholarly law review articles more thoroughly address the Law of War implications of cyber operations. They focus on how to conduct cyber operations in compliance with the Law of War. Often, they lack the factual details that investigative campaign analyses include, using only the minimum amount of facts necessary to make their legal arguments. While this is a norm in legal writing and helps frame legal rules, it does not necessarily guide the practitioner through the shadows of real-life variations.

Much about how the Law of War applies to cyber and space operations remains unsettled. Significant questions are still actively being debated by scholars and states alike. Some of these questions include: What is a cyber attack? Do all cyber operations amount to a use of force or act of aggression under article 2(4) of the U.N. Charter? Do they amount to armed attack under article 51 of the U.N. Charter? Is data an object? Should cyber and space infrastructure be treated as a protected class (similar to hospitals) to give the Law of War meaning in terms of minimizing suffering to civilians? Is space a global common? States (to the extent they have articulated a position) and scholars alike come down on different sides of each of these questions.[14]

U.S.C. § 3093(e). Of note, however, political science research discussing the escalation and deterrence impacts of cyber operations and comparing them to kinetic operations' escalatory and deterrent effects demonstrates that cyber operations do not have the same escalatory effect as kinetic operations. *See generally* BENJAMIN JENSEN & BRANDON VALERIANO, ATL. COUNCIL: SCOWCROFT CTR. FOR STRATEGY AND SEC., WHAT DO WE KNOW ABOUT CYBER ESCALATION? OBSERVATIONS FROM SIMULATIONS AND SURVEYS (2019), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/what-do-we-know-about-cyber-escalation-observations-from-simulations-and-surveys/ [https://perma.cc/3354-83PV] (demonstrating that cyber operations do not have the same escalatory effect as kinetic operations).

14 *Compare* Sean Watts & Theodore Richard, *Baseline Territorial Sovereignty and Cyberspace*, 22 LEWIS & CLARK L. REV. 771, 771 (2018) (examining "emerging State cyber practice" and legal views surrounding the application of State sovereignty to cyberspace), *with* Noah Weisbord, *Judging Aggression*, 50 COLUM. J. TRANSNAT'L L. 82, 152 (2011) (arguing for clear judicial standards regarding what constitutes an "armed attack"), *and* Andrew Moore, *Stuxnet and Article 2(4)'s Prohibition Against the Use of Force: Customary Law & Potential Models*, 64 NAVAL L. REV. 1, 2 (2015) (addressing "the customary inter-

Unfortunately, due to the inherent secrecy associated with cyber and space operation capabilities, many state policies and positions remain classified or unstated. When coupled with the twin difficulties of attribution and private/non-state actor operations, discerning state practice is often a murky enterprise. Consequently, amongst the literature on the topic, there is a disproportionate amount of scholarly debate as compared to historical Law of War developments, where states have traditionally led the debate, with scholars filling in the gaps. With states declining to weigh in with authoritative positions—or stating very general positions—researchers are left citing high-ranking legal advisors' unclassified speeches as authoritative.[15] Examples of these include: Harold Koh's (Department of State Legal Advisor) speech at the U.S. Cyber Command (CYBERCOM) legal conference,[16] Brian Egan's (Department of State Legal Advisor) speech at the Berkeley Center for Law and Technology,[17] and Roy Schondorf's (Israeli Deputy Attorney General) speech at the Stockton Center for International Law.[18] Often, these legal advisors opine on some of the critical questions listed above, but other states do not, leaving the researcher with only one state's position—hardly enough to deduce a norm.

The *Tallinn Manual 2.0* represents the widest-ranging application of international law to cyber and space operations.[19] It

---

pretation of force prohibited by Article 2(4)" of the U.N. Charter), *and* Peter Pascucci, *Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution*, 26 MINN. J. INT'L L. 419, 422 (2017) (analyzing international humanitarian law regarding distinction and proportionality in cyberwar).

15 *See generally* Scott Sullivan, *Toward Clarity in Cyber's "Fog of Law*,*"* 10 CYBER DEF. REV. 59 (2025) (highlighting the persistent and intentional ambiguity surrounding legal positions on state-sponsored cyber operations).

Unclassified speeches are not an abnormal source for Law of War developments but, because these speeches are inherently generic, when they are the only source and are made few and far between, they tend to be less useful for discerning a developing norm.

16 Harold Hongju Koh, Legal Advisor, U.S. Dep't of State, International Law in Cyberspace (Sep. 18, 2012), https://2009-2017.state.gov/s/l/releases/remarks/197924.htm [https://perma.cc/4LYK-LTJE].

17 Brian J. Egan, Legal Advisor, U.S. Dep't of State, Remarks on International Law and Stability in Cyberspace (Nov. 10, 2016), https://2009-2017.state.gov/s/l/releases/remarks/264303.htm [https://perma.cc/K2VQ-43VR].

18 Roy Schondorf, Israeli Deputy Att'y Gen. (Int'l Law), Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations (Dec. 9, 2020), https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/ [https://perma.cc/8DS2-CJVX].

19 *See generally* INT'L GRP. OF EXPERTS, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017) [hereafter TALLINN MANUAL 2.0] (explaining the scope of how international law governs cyber operations).

is the widest-ranging because it is both the most thorough and includes the most diverse group of international contributors.[20] The trouble, as every practitioner (especially Americans) is quick to point out, is that the *Tallinn Manual 2.0* is neither a treaty nor has it been adopted by any state as an authoritative statement of the law.[21] It is a consensus view of experts, not a *jus cogens* norm carrying the weight of law.[22]

Finally, legal writing in general addresses whether the object of a cyber operation is a military object or a civilian object, but very little of this literature addresses the implications of military use of cyber and space infrastructure and the impacts that use may have on its classification as a lawful target. This may be because, under the Law of War, cyber and space infrastructure is like any other dual-use object; targetable assuming it complies with the other Law of War requirements. This may also be because there are few articulable norms regarding cyber operations. One that does appear to be nascently developing is that cyber operations in and of themselves do not merit kinetic responses. Or put another way, only cyber responses are proportionate to cyber operations. Whether that is a *jus cogens* legal norm that is forming (doubtful) or a political decision about escalation and deterrence (most likely) remains to be seen. The one point most of the legal writing agrees on is that cyber and space weapons are in fact subject to the Law of War.

---

20 The lists of contributors span eleven pages and includes representation from many countries, academics, military practitioners, and government employees. *Id.* at xii–xxii. The group is largely western, though some contributors hail from Japan and China. *See id*. No doubt this is due to it being a product of an International Group of Experts hosted by NATO's Cooperative Cyber Defence Centre of Excellence. *Id.* at iv.

21 Nonetheless, in breadth, depth, substance, format, explanatory comments, and thoroughness, the *Tallinn Manual 2.0* is essentially a Restatement of Law, which in every other field of law is a foundational starting point. *See* Michael Schmitt, *Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't*, JUST SEC. (Feb. 9, 2017), https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/ [https://perma.cc/7PXB-HKCG]. Every jurisdiction varies slightly from the Restatement, but it is generally a reliable statement of the law. *Id.* The very fact of most practitioner's reluctance to endorse the *Tallinn Manual 2.0* (despite having a copy on their desks) is in and of itself a commentary on the state of the Law of War as it applies to cyber operations.

22 *Jus Cogens*, BLACK'S LAW DICTIONARY (9th ed. 2009) ("A mandatory or peremptory norm of general international law accepted and recognized by the international community as a norm from which no derogation is permitted.").

III. HYPOTHETICAL SCENARIO: CYBER CASCADE[23]

The year is 2026 and the political tensions in the South Asian Sea that have been rising for the past 30 years are at a fever pitch. The Hague's Permanent Court of Arbitration recently ruled that State A had no legal claim to the Johnson Atolls, a series of maritime features in the South Asian Sea that do not qualify as islands.[24] The Johnson Atolls are in the Exclusive Economic Zone (EEZ) of State B, a relatively underdeveloped military power.[25] State A continues to develop military infrastructure on these non-island features. While tensions are high, States A and B remain at peace. State A operates airborne intelligence, surveillance, and reconnaissance (ISR) platforms from the Johnson Atolls—both manned and unmanned—and conducts regular resupply missions to the atolls. In addition to the ISR systems in the Johnson Atolls, State A regularly patrols the area with warships that harass State B commercial activity (fishing and oil drilling), and scrambles fighter jets to intercept any aircraft that enters what State A claims is national airspace above the Johnson Atolls.[26]

State C, a major world power, is a treaty ally with State B. State C launches a complex cyber operation, codenamed CASCADE, that uses Stuxnet-like technology to worm its way through cyberspace and is specifically designed to identify air traffic control (ATC) and air defense systems utilized by State A

---

23 The scenario presented in this section is a hypothetical cyber operation based on historical cyber operations and publicly available information. Every effort has been made to use realistic components of historical examples to identify that these are realistic possibilities today, rather than futuristic ideas.

24 An island is defined as "a naturally formed area of land, surrounded by water, which is above water at high tide" and can sustain human habitation or economic life of its own. *See* U.N. Convention on the Law of the Sea art. 121, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS]; DEP'T OF THE NAVY, NWP 1-14M, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 1-7 (2022) [hereinafter NWP 1-14M]. Each island has its own territorial sea, contiguous zone, and exclusive economic zone. *Id.* N.B.: While the United States has not ratified UNCLOS, it played a major role in the negotiation process, and the U.S. position is that these provisions are consistent with customary international law. *See* Off. of the Staff Judge Advoc., U.S. Indo-Pac. Command, *The U.S. Position on the U.N. Convention on the Law of the Sea*, 97 INT'L L. STUD. 81, 82–83 (2021); Presidential Statement on United States Oceans Policy, 19 WEEKLY COMP. PRES. DOC. 383 (Mar. 10, 1983).

25 The EEZ is defined as "an area beyond and adjacent to the territorial sea," out to "200 nautical miles from the baselines," in which the coastal state has exclusive and sovereign rights for the purpose of exploring and exploiting, conserving and managing the natural resources. UNCLOS, *supra* note 24, arts. 55–57. Of note, it includes the rights and jurisdiction over "the establishment and use of artificial islands." *Id.* art. 56.

26 National airspace is that airspace superjacent to "the State's territory, internal waters, territorial sea, and, in the case of an archipelagic State, archipelagic waters." NWP 1-14M, *supra* note 24, at 2-16.

on the Johnson Atolls.[27] In searching for the targeted systems, CASCADE moves through various communications networks, largely privately owned, passing through both computer networks and communication satellite constellations that provide internet services. When CASCADE identifies that a particular terminal is not a targeted system, it deletes itself from the system and continues its hunt. Once CASCADE identifies the target systems, it notifies the sender, and after a built-in delay period of several months, it deploys its payload.

CASCADE's payload is designed to erase all data on the target systems. By doing so, the ATC systems used to ensure safe flight operations are rendered inoperable, causing a State A military unmanned ISR aircraft to crash into one of the airfields on the Johnson Atolls, causing significant damage to the infrastructure and destroying the aircraft. Several State A manned military ISR aircraft had to divert and conduct emergency landings in State B's sovereign territory, initiating what is becoming a protracted dispute between State A and B over the return of the pilots and aircraft.

Because State A has developed a significant cyber force capability over the last ten years, it is able to relatively quickly identify CASCADE, build countermeasures that prevent it from causing further damage to State A systems, and identify several Amazon Web Service (AWS) data center sites in State C and specific commercial satellite constellations that CASCADE passed through while searching for the targeted systems.[28] State A was not able to directly attribute CASCADE to State C; however, State A has nonetheless publicly blamed State C for the CASCADE attack, arguing that, because of State C's level of sophistication, State C either conducted the attack itself or knew

---

27 For an in-depth case study of Stuxnet, see generally ZETTER, *supra* note 9. A worm is a type of computer program that is difficult to detect, self-replicates, burrows deep into computer systems, and rapidly spreads across networks. *See id.* at 13.

28 AWS has hundreds of data centers in countries all over the world. *See AWS Global Infrastructure*, AMAZON WEB SERVS., https://aws.amazon.com/about-aws/global-infrastructure/https://aws.amazon.com/about-aws/global-infrastructure/ [https://perma.cc/XT5H-3PBW] (last visited Sep. 29, 2025). AWS is used in this hypothetical simply because the majority of its data transactions are presumptively commercial and civilian. *Id.* Furthermore, because of the breadth of AWS's physical international presence, it provides an element of placement and access. *Id.* Google or Microsoft would just as easily make the point. *See, e.g.*, *Discover Where the Internet Lives*, GOOGLE: DATA CTRS., https://www.google.com/about/datacenters/locations/ [https://perma.cc/Q7AA-GR2H] (last visited Sep. 29, 2025); *The Backbone of Microsoft Cloud: Our Datacenters*, MICROSOFT DATACENTERS, https://datacenters.microsoft.com [https://perma.cc/Q3RR-K93H] (last visited Sep. 29, 2025).

the attack was conducted from its infrastructure and was unwilling or unable to prevent it.

Consequently, State A views CASCADE as an act of war, and conducts a missile strike on one of the data centers in State C and uses an anti-satellite missile against a commercial satellite internet constellation. The strike on the data center kills approximately 300 civilian employees and destroys servers that many companies rely on for secure data storage and cloud support. The strike on the satellite constellation destroys several satellites and creates a massive field of space debris in low Earth orbit. Several other countries' national and commercial satellites are damaged by the resulting space debris.

While not directly attributed to State C, State A claims that the strike was in self-defense and that it was lawful, given State C's advanced cyber capability and apparent unwillingness to prevent cyber attacks from passing through its cyber and space infrastructure. Further, State A claimed self-defense because CASCADE was still active in cyberspace, seeking additional systems that meet the target criteria—systems that State A relies on in other parts of the South Asian Sea.

IV. LAW OF WAR FOUNDATIONS AND CYBER AND SPACE IMPLICATIONS

A. General Rules Defined

There are five foundational Law of War principles: military necessity, distinction, proportionality, humanity (or avoiding unnecessary suffering), and honor.[29] There is a host of nuance to each principle and whole treatises have been written about each individually. This section expounds the basic rules with a focus on how they manifest in the cyber and space domains. In the interests of relevance and brevity, this scenario focuses on the principles of military necessity, distinction, and proportionality. While humanity and honor remain relevant to all aspects of armed conflict, they are beyond the scope of this Article. These principles are part of the subset of International Law known as the Law of War or the Law of Armed Conflict (LOAC). The Law

29 OFF. OF GEN. COUNS., DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL § 2.1.2.3 (2023) [hereinafter DOD LAW OF WAR MANUAL]. Note that while honor is included in the DoD Law of War Manual, it is not always enumerated as a core principle. *See, e.g.*, SOLIS, *supra* note 8, at 209–45; GEOFFREY CORN ET AL., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 112 (1st ed. 2012); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78 (July 8).

of War is a *lex specialis*, which means it only applies to armed conflicts, and it supersedes other bodies of law during armed conflicts.[30]

The principle of military necessity justifies the conduct of war: killing and destroying both people and property. It "justifies the use of all measures needed to defeat the enemy as quickly as possible" so long as those measures are not otherwise prohibited by the Law of War.[31] Simply put, military necessity is what justifies violence. While distinct, there is a natural and inherent consistency here with self-defense doctrines requiring that force be a last resort, i.e., that it be necessary to mitigate the threat.[32] While naturally consistent with self-defense in a *jus ad bellum* context, military necessity is not an admission ticket—useful for getting into a war, and then cast aside. It remains applicable for the duration of the conflict. Military necessity affirmatively justifies offensive operations in a *jus in bello* context and imposes a corollary restriction: killing and destruction that are not militarily necessary are prohibited. It is a requirement that the conduct be necessary.

Because the Law of War principles evolved with war in mind—indeed, that is their reason for existing—they account for the exigencies of war.[33] In other words, the concept of military necessity recognizes and assumes certain types of military actions are inherently necessary.[34] It does not, however, justify unnecessary, wanton destruction: destruction for destruction's sake, killing for killing's sake. Such an interpretation defies the meaning of the word *necessity* and guts the principle wholesale.

The principle of distinction is the hallmark of a professional military. Essentially, it stands for limiting the *intentional* effects of war to military objectives. The principle imposes a two-fold requirement. First, it requires belligerents to attack only the enemy, as opposed to civilian populations and other protected persons and objects.[35] Second, it requires belligerents to distinguish themselves from non-military persons and objects.[36] Significant

---

30 WILLIAM WINTHROP, MILITARY LAW AND PRECEDENTS 773 (2d ed. photo. reprt. 1920) (1896); DOD LAW OF WAR MANUAL, *supra* note 29, § 1.3.2.1.

31 DOD LAW OF WAR MANUAL, *supra* note 29, § 2.2.

32 *Compare id.* § 1.11 (explaining *jus ad bellum* criteria), *with id.* § 2.2 (explaining military necessity).

While consistent, § 1.11.1.3 makes clear that "The *jus ad bellum* criterion of *necessity* is different from the *jus in bello* concept of *military necessity*." *Id.* § 1.11.1.3.

33 *Id.* § 2.2.2.1.

34 *Id.* § 2.2.3.2.

35 *Id.* § 2.5.2.

36 *Id.* § 2.5.3.

implications flow from these two requirements, and civilian objects are presumed as non-military without a requirement of any distinctive sign, placing the onus on the belligerent militaries to discriminate between civilian and military.[37]

In simple terms, the principle of proportionality is a balancing test: incidental harm cannot be excessive when weighed against the concrete and direct military advantage to be gained by an attack. Accordingly, belligerents are obligated to refrain from attacks that cause excessive collateral harm, when that collateral harm is not outweighed by the military advantage to be gained. Proportionality also requires belligerents to take "feasible precautions" to minimize collateral damage.[38] The analysis of proportionality is inherently subjective and can have nearly infinite variations. What was acceptable incidental harm fifty or one hundred years ago, may not be lawfully acceptable today, given what is technologically feasible today.

The principle of proportionality injects the age-old legal standard of reasonableness into the notion of military necessity. While killing and destruction are lawful in war, it must not be unreasonable or excessive. The principle is distinct from *jus ad bellum* self-defense proportionality, which limits the use of force to the amount required to mitigate the threat. In war, incidental destruction of civilian property and civilian casualties—often referred to as collateral damage—are tragic, but are expected and accepted as inevitable.[39] Just as military necessity is not license for unnecessary destruction, it is not license for excessive, unreasonable collateral damage either.

Proportionality has taken a distinctive predominance in the post-World War II era, especially with the advent of Additional Protocol I in 1977.[40] Nonetheless, the notion of minimizing collateral damage is not a new concept, though the weighing of it against military necessity is relatively modern. Hugo Grotius wrote, "As for the killing of persons who are slaughtered incidentally, without intention, . . . except for grave reasons affecting the safety of multitudes, nothing should be done that may

37 SOLIS, *supra* note 8, at 209–10.

38 DOD LAW OF WAR MANUAL, *supra* note 29, § 5.10.

39 *Id.* § 2.4.1.2.

40 Protocols Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts, arts. 50–58, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].

threaten the destruction of innocent people."[41] Historically, the concept of minimizing collateral damage has been discussed as a subset and outgrowth of distinction, rather than a separate principle as it is today. This evolution reflects the technological growth of weapons capable of killing and destroying in a disproportionate manner and so proportionality has grown into a standalone principle in its own right.[42]

B. Specific Implications for Cyber and Space

Cyber and space operations, like all military operations, can range on a spectrum from defensive operations to reconnaissance operations to offensive operations. This includes passive information and data collection operations, akin to any spying activity that has existed as long as war itself, and active measures using 1s and 0s in the virtual world to cause actual destruction in the physical world. Since cyber and space operations are not always as clear as kinetic military operations, it is helpful to tease out specific implications for how the Law of War applies in cyberspace.

First, it is an accepted norm that international law applies in cyberspace.[43] Stated inversely, cyberspace is not a lawless realm where state sovereignty and international law has no reach (as advocated in the early days of the internet.)[44] So, the principles discussed above apply to cyber operations during armed conflict.[45]

Second, a cyber operation may amount to a use of force under article 2(4) of the United Nations (U.N.) Charter. The *Tallinn Manual 2.0* defines a cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[46] The *Tallinn Manual 2.0* adopts the definition of attack found in Additional Protocol I, which means violence against an adversary,

41 HUGO GROTIUS, THE LAW OF WAR AND PEACE 353 (Louise R. Loomis, trans., Classics Club 1949) (1625). *See generally id.* ch. XI–XII (explaining when killing is permitted in lawful wars and the situations that allow for the destruction of another's property).

42 GEOFFREY BEST, WAR AND LAW SINCE 1945, at 323–24 (1994).

43 Koh, *supra* note 16; TALLINN MANUAL 2.0, *supra* note 19, at 16 ("Rule 3 – External sovereignty[.] A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it."); *id.* at 375 ("Rule 80 – Applicability of the law of armed conflict[.] Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict.").

44 *See generally* THOMAS RID, RISE OF THE MACHINES: A CYBERNETIC HISTORY (2016) (explaining the history of the rise of the internet and the cultural debate about whether the law generally had any effect in cyberspace).

Harold Koh responded to this question with the now-accepted international norm: "Emphatically no. Cyber space is not a 'law-free' zone." Koh, *supra* note 16.

45 DOD LAW OF WAR MANUAL, *supra* note 29, §§ 16.2, 16.5.

46 TALLINN MANUAL 2.0, *supra* note 19, at 415.

whether offensive or defensive in nature.[47] Doing so eliminates non-violent military operations (e.g., psychological or cyber espionage) from the definition of a cyber attack. Further, this definition is effects-focused, as the definition of a use of force generally is in international law.[48] There is also an element of causation that is necessary: did the cyber operation proximately result in death, injury, or significant destruction? If so, it would constitute a use of force.[49] Ultimately, if the cyber operation causes physical consequences that a kinetic operation would cause, the cyber operation should equally be considered a use of force.[50]

There is an open debate about whether the destruction of data—vice physical destruction of the computers—constitutes an attack. There are valid arguments on both sides of the debate. An example is illustrative here. A scenario in which the destruction of international exchange data that causes no physical destruction would not constitute an attack under the Law of War, despite the widespread and long-term economic harm that would surely follow. To some, this hardly seems reasonable given that the purpose of the Law of War is to protect bystanders from the effects of war.[51] On the other hand, the lack of physical destruction does not satisfy the requirement of violence that seems inherent in the meaning of the word attack when discussing the Law of War. Further, a cyber operation that involves a psychological campaign to erode confidence in a market, without actually doing anything to the objective data, could cause as much damage as the data-destroying cyber operation, making this an even thornier problem to weigh. In essence, a state could achieve the same effects through different means, and one would constitute an armed attack under the Law of War and the other would not. Ultimately, whether destruction of data constitutes a use of force depends on the circumstances: did the destruction of data proximately cause physical effects? If so, then it is a use of force; if not, then it is not a use of force.[52]

---

47 AP I, *supra* note 40, art. 49; *see* THE JUDGE ADVOC. GEN'S. LEGAL CTR. & SCH., NAT'L SEC. L. DEP'T, LAW OF ARMED CONFLICT DOCUMENTARY SUPPLEMENT 214, 249–51 (2022) (outlining how the United States signed the AP I, but did not ratify it, and explaining the portions of the AP I the United States considers customary international law).

48 Koh, *supra* note 16.

49 *Id.*

50 *Id.*; *see also* TALLINN MANUAL 2.0, *supra* note 19, at 330 ("Rule 69 – Definition of use of force[.] A cyber operation constitutes a use of force *when its scale and effects are comparable to non-cyber operations* rising to the level of a use of force." (emphasis added)).

51 Pascucci, *supra* note 14, at 460.

52 *Id.* at 437–38. If not a use of force, and the Law of War does not apply, that does not necessarily make the conduct lawful—it is just subject to a different legal regime.

But that is the crux of the issue. Violence actually matters in the law. Persuasion in the cognitive realm is legitimate, force in the physical realm (when unlawful) is not. Data lies somewhere in the middle. Because of this dilemma and the centrality of data to the modern world, some argue that data should be given a protected status, similar to hospitals and cultural property.[53] Still others argue that the principles of distinction and proportionality adequately limit a state's ability to wreak such widespread and long-lasting catastrophic damage.[54]

The principle of distinction equally applies to cyber operations. The secondary requirement of distinction is that militaries should distinguish themselves from civilians. While attribution is written about extensively, the relation of cyber operations to the concept of distinction appears only tangentially. Yet, attribution is one of the biggest problems of cyber operations because the target of the operation cannot distinguish whether the perpetrator of the cyber operation is a civilian or a military entity. Code does not wear a uniform. Often the nature of the cyber operation is indicative, but not always.[55] Take the North Korean cyber operation against Sony Pictures prior to the release of the movie *The Interview*, for example. There a state actor targeted a civilian entity, but not for a military-related purpose. For an even more poignant example, take the case of Jonathan James, a private citizen who, in 1999 at the age of fifteen, hacked into Department of Defense and NASA systems.[56] While neither of these examples constitute a use of force, they demonstrate the point that indi-

---

53 *Id.* at 458–60 (advocating the adoption of an Additional Protocol affording data a protected status).

54 *Id.* at 419, 430. This author's position is that if the principles of distinction and proportionality are insufficient to address these kinds of concerns, an additional protection of naming data a protected class is not going to have any efficacy. Further, a blanket protection of data would be too broad and eliminate many legitimate military targets—intelligence data, for example.

55 It remains a largely unanalyzed question whether cyber operations that amount to a use of force but do not distinguish themselves as military actors violate the principle of distinction. Traditional applications of distinction indicate this would be a violation, and at the same time, the covert nature of these operations tend to make them more analogous to espionage-like acts of sabotage. Furthermore, the law will not require states to leave a calling card of sorts to identify their cyber weapons as military. Hence, this aspect of distinction largely remains a deductive analysis based on the nature of the act. By way of comparison, a bomb dropped from a plane is rarely identified explicitly as being dropped by a military actor vice a civilian actor, and yet, that does not violate the principle of distinction because of the nature of the attack is presumptively military. Because this is a topic that exceeds the scope of this Article, it will not be addressed more thoroughly.

56 Vilius Petkauskas, *How a Florida Teenager Hacked NASA's Source Code*, CYBERNEWS (July 28, 2023), https://cybernews.com/editorial/how-a-florida-teenager-hacked-nasas-source-code/ [https://perma.cc/2WSC-YSAJ].

and non-state actors both conduct and are targeted by cyber operations that easily could lead to a use of force.

Here, it bears mentioning that the Law of War has traditionally tolerated covert actions in the form of espionage without finding a violation of this aspect of distinction. That is, the Law of War does not forbid such actions (even though the actor is often trying to blend in with a civilian population), however, the consequence if caught is that the individual actors forfeit any protected status they may have had as combatants. They surrender themselves to the laws of the country against which they are taking an action. Historically, this has meant peremptory execution. Because cyber operations in many ways afford countries the opportunity to engage in these espionage-like covert actions without ever placing a person within the physical jurisdiction or control of the opposing country, cyberspace enables covert actions without the risk of physical capture. Accordingly, cyber tools that are intended to look harmless and be accepted by the target system are not violations of the principles of distinction nor perfidious in nature.[57] In essence, they are more akin to the Trojan Horse than to a combatant failing to distinguish himself from the civilian population or abusing a protected symbol to do violence.

Finally, and worth noting, cyberspace is not a public common, like international waters or airspace. A missile flying through air, does not make the airspace dual-use—it is occupying a piece of physical space for a period of time. But a cyber weapon flying through cyberspace is a weapon flying through (or dwelling in) privately owned infrastructure, which is materially different. The owner may not have consented to that use of the infrastructure. Indeed, the owner may not have even known that it occurred. Nonetheless, a military sending a cyber weapon through privately owned infrastructure, has potentially turned that infra-

---

57 Perfidy is the illegal use of a protected class or symbol (e.g., acting wounded, or wearing the red cross, or using a white flag to lure enemy combatants in) specifically to kill, injure, or capture the enemy. *Perfidy*, INT'L COMM. OF THE RED CROSS, https://casebook.icrc.org/a_to_z/glossary/perfidy [https://perma.cc/ABZ8-3GCW] (last visited Nov. 7, 2025). This is a customary rule of the Law of War that has been incorporated into AP I. *See* AP I, *supra* note 40, art. 37 ("It is prohibited to kill, injure, or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obligated to accord, protection under the rules of international applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy."); *see also* SOLIS, *supra* note 8, at 350–66 (discussing how perfidy is a violation of LOAC and might be a grave breach).

The United Kingdom Manual of the Law of Armed Conflict and the DoD Law of War Manual adopt the same language. MINISTRY OF DEF., THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT §§ 5.9–.10 (2004); DOD LAW OF WAR MANUAL, *supra* note 29, §§ 5.21–.24.

structure into a dual-use object subject to lawful destruction. This is materially different from the sea, land, and air domains. Cyberspace is not a naturally occurring physical thing, like the electromagnetic spectrum, air space, outer space, or the ocean. It is a man-made thing owned by many people and companies.

V. PROPOSED ANALYTICAL FRAMEWORK

A. What a Framework Must Do

Analytical frameworks come in all shapes and sizes, and with varying names and degrees of usefulness. It is helpful to identify who it is intended for and to define what an analytical framework should do.

The target audience for this kind of analytical framework is military commanders and military legal advisors who often have to make decisions under pressure, with limited time, and without complete information. While these circumstances help shape how to think about such a framework, they do not limit the use of the framework to rapid response scenarios—the framework should also serve the function of enabling prudent planning. An inquisitive outline that promotes analysis for the sake of deeper understanding, while valuable, is not necessarily helpful in this situation, though using one can help a decision maker ensure she is not missing vital pieces of information that create gaps in understanding.

For an analytical framework to be useful, it should meet certain criteria. It should facilitate decision making or prudent planning. It should be simple enough to work through in a time-constrained environment. It should enable comprehensive decisions. It should account for minority or outlier data points and ascribe appropriate weight to them. An analytical framework need not be innovative. It need not prescribe previously unused elements or factors. It need not propose changes to the existing law (and if the intent is problem solving, it arguably should not). An analytical framework can be as simple as a checklist of elements, like those often used by television prosecutors. It can be as complicated as an if-then flow chart that accounts for multiple variables.

For purposes of responding to a problem set like a strike on a known belligerent during an international armed conflict, it could be a simple listing of Law of War principles plus additional operational authorities, like rules of engagement. For a more complex problem set, like the CASCADE hypothetical, something

more robust is advisable—even for a commander or legal advisor who is very comfortable with the Law of War and has a strong background working through these types of problems. For the novice legal advisor, something more robust is advisable even for the simpler tactical problems. Frameworks inject discipline into legal analysis. They ensure consistency. Finally, from a practical perspective, this Article recommends turning the framework into a worksheet that practitioners can use as they analyze problems. See Appendix A for an example.

B. Proposed Framework

The following is a proposed framework for assessing kinetic targeting of cyber and space infrastructure. Because of the nature of it as a dual-use object, there will be a significant amount of discussion focusing on proportionality and distinction. Figure 1 graphically outlines a proposed analytical framework. Subsequent subsections explain the framework in detail. Part VI will apply the framework to the CASCADE hypothetical.

Figure 1

Does the Law of War Apply?	• The Law of War is a *lex specialis* that applies only to armed conflicts. • Is there an armed conflict? International or non-international? • Does the cyber operation constitute a use of force?
Distinction	• Is it an inherently military person or object? • Is it a military object by its nature, use, location, or purpose?
Proportionality	• Identify collateral effects • Identify military advantages to be gained • Balance • Identify feasible precautions to mitigate potential collateral damage • If dual-use: ○ Is it predominantly military or predominantly civilian? If predominantly civilian, when assessing proportionality, the military interest must be commensurately greater. (i.e., the greater the collateral effects, the greater the military advantage to be gained must be.)
Operational Authorities	• Does your commander have the operational authorities in an EXORD or OPORD to conduct the operation? • Do the Rules of Engagement permit the operation? • If not, at what level is the approval authority? • Authority at the right time? In the right place? For the right target? For the right weapon?

Does the Law of War Apply? This step may seem elementary, and, depending on the context, may not be necessary. But it is critical. As a *lex specialis*, the Law of War only applies to armed conflict—whether it is an international or non-international armed conflict will determine which portions of it apply and how. As an initial step, determining whether there is an armed conflict matters. In a *jus in bello* context, whether an armed conflict is occurring will be apparent and already established. In a *jus ad bellum* assessment, however, whether an armed conflict is beginning will hinge on whether an act constitutes a use of force and possibly even how a nation responds to that use of force. This need not be a cyber operation, though it could be.

Does the cyber operation constitute a use of force? This Article is predominantly focused on the kinetic targeting of cyber and space infrastructure. Plenty has been written and said about what constitutes a use of force in cyberspace. Despite the focus of this Article, whether a cyber operation constitutes a use of force is still relevant to the assessment of a lawful response. If it is not a use of force, there is no justification for a forceful response in self-defense.[58] Accordingly, whether a cyber or space operation constitutes a use of force matters in both *jus in bello* and *jus ad bellum*.

Distinction. The basic principle of distinction is outlined above. More practically though, how is one to distinguish between military and non-military persons/objects? The test for determining if a person or thing is a military objective is whether by its inherent nature (e.g., a fighter jet or a soldier), location, purpose, or use (e.g., using a normal pickup truck as a military vehicle), it makes an effective contribution to military action.[59] Because "use" is the most relevant to this discussion, that will be the focus of analysis here, to the exclusion of nature, location, and purpose (in another context any of those may be the focus).

---

58 *See* DOD LAW OF WAR MANUAL, *supra* note 29, § 1.11.5.2 (explaining that the United States views any illegal use of force as sufficient to invoke the right of self-defense, but many states draw a finer distinction between uses of force and "armed attack[s]").

Because this distinction elevates when a state may respond in self-defense, it actually has the effect of permitting some degree of force and requires states to accept it. *Id.* In fact, this distinction encourages the low-level uses of forces that do not cross the armed attack threshold. *Id.* While this Article has adopted the use of force threshold, the *Tallinn Manual 2.0* draws a distinction between use of force and armed attack (perhaps a reason why many American practitioners are quick to note the limitations of the *Tallinn Manual 2.0*). TALLINN MANUAL 2.0, *supra* note 19, at 37.

59 DOD LAW OF WAR MANUAL, *supra* note 29, § 5.6.3.

> "Use" refers to an object's present function. For example, using an otherwise civilian building to billet combatant forces makes the building a military objective. Similarly, using equipment and facilities for military purposes, such as using them as a command and control center or a communications station, would result in such objects providing an effective contribution to the enemy's military action.[60]

Accordingly, there is a temporal quality to "use" as a test for whether an object is a military object. Its use must be present. Now, if an object is routinely militarily used, the need for present use diminishes. Whether one-time use of a building, for example, is sufficient to make it a military object for the remainder of the conflict, however, is a less certain thing. And that is where the definite military advantage to be gained comes into the analysis.

Whether there is a definite military advantage to be gained is assessed at the time of the proposed strike, "in the circumstances ruling at the time."[61] If the building is intermittently used and it is likely to be used accordingly throughout the conflict, then under those circumstances, its destruction would offer a military advantage, and it would be considered a military object. If, however, it was used one time, several months ago, it is significantly less likely that the destruction of such a building would offer any military advantage. The same is true of cyber and space infrastructure: the circumstances ruling at the time, as well as the context of the conflict to date, matter.[62]

"Dual-use" as a term is descriptive, rather than a specific legal regime or term of art. From a legal perspective, dual-use is not a category: objects are either military objects lawfully subject to attack or they are not.[63] Indeed, some scholars eschew the use of the term altogether because the dual-use nature of an object "d[oes] not alter its singular and unequivocal status as a military

---

60 *Id.* § 5.6.6.1.

61 *Id.* § 5.6.7.2 (noting that "definite" means concrete and perceptible, not speculative or hypothetical); *id.* § 5.6.7.3.

62 In the context of whether a person is a military objective or not, the discussion analogous to dual-use is that of direct participation in hostilities (DPH). Much ink has been spilled discussing whether and when a civilian is directly participating in hostilities and the consequences of that participation. While the United States has rejected a so-called "revolving door" theory of DPH, there has been shockingly little discussion about when an object becomes dual-use and the persistence of that status through intermittent use. *See id.* § 5.8.4.2; NILS MELZER, INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 70 (2009); SOLIS, *supra* note 8, at 191–94. This is likely due to the fact that the destruction of objects often (and rightly) receives less scrutiny than the killing of people. DPH is largely beyond the scope of this Article, since cyber operations typically target objects.

63 DOD LAW OF WAR MANUAL, *supra* note 29, § 5.6.1.2.

objective."[64] The problem of dual-use objects is two-fold. It is both a distinction problem and a proportionality problem. In terms of distinction, under a plain reading of the law, the dual-use problem is easier to resolve. If it serves a military purpose, and the destruction of it would offer a military advantage, it is a military object.

Proportionality. It is easy to articulate the analysis for proportionality. Applying it in the real world, however, is another matter. It is fraught with value judgments and subjectivity—as are most command decisions. Frequently second-guessed and deconstructed by pundits and higher headquarters alike, proportionality is often the murkiest of all the principles of the Law of War.[65] Providing an additional layer of confusion, the same word is used in two legal concepts: Law of War proportionality and self-defense proportionality—both of which must be discussed here. Proportionality as a self-defense concept is relevant here in a *jus ad bellum* context.

When it comes to dual-use objects—especially infrastructure—proportionality becomes more complicated than the simple recitation. In plain terms, the Law of War requires the identification of the military advantage to be gained, the identification of potential collateral damage and implementation of feasible precautions to minimize such collateral damage, and then the weighing of the two. No mathematical precision is required. It cannot and should not be reduced to a comparison of quantity of enemy troops killed versus quantity of potential civilian casualties. Value judgments are inherent in this process.

Some factors to consider, depending on the facts and circumstances, during this stage in the analysis include the following questions: What is the gravity of the military advantage to be gained—is this likely to be a war ending strike, or a routine strike? Will a combination of fusing and precision guided munitions minimize collateral damage? Will the timing of the strike minimize collateral damage? Will the opportunity be lost if waiting for less collateral damage? Is the target mobile? Was the target intentionally placed by protected objects—placing a command and control center right next to a hospital, for example? How

64 Yoram Dinstein, *Discussion: "Dual-Purpose" Targets*, 78 INT'L L. STUD. 218, 218–19 (2002).

65 Anaïs Maroonian, *Proportionality in International Humanitarian Law: A Principle and a Rule*, LIEBER INST. AT WEST POINT (Oct. 24, 2022), https://lieber.westpoint.edu/proportionality-international-humanitarian-law-principle-rule [https://perma.cc/5MZ8-M665] (explaining the dual role of proportionality as both a foundational principle and an enforceable rule in international humanitarian law).

much data is stored or transmits through the data center? Is data actually stored there, or is it a transit hub? Is that data predominantly civilian in nature or military? Recency, quantity, and duration of both military and civilian uses of the target are all relevant. Is a lesser means of achieving the same military advantage available? That is, would simply disrupting or degrading the data center accomplish the same effect needed for the military goal, or is actual destruction required? And, importantly, what is the feasibility of that lesser means?

Often when advising on proportionality questions, using historical examples help paint the picture of acceptable precautions and a balanced approach—to gain both a sense of what precautions the law expects and of what constitutes proportionality in real terms.[66] During the 1991 Gulf War, coalition forces targeted the Iraqi integrated power grid that generated and distributed electrical power to both civilian and military entities.[67] Because it supported military entities including anti-air radars and command and control capabilities, the power grid itself was a lawful military objective.[68] The incidental impacts on the civilian population made it a proportionality issue rather than a distinction issue. The NATO campaign in Kosovo provides an illustrative example of feasible precautions. In attacking the integrated electrical power stations that serviced both civilian and military entities, rather than destroying the power stations, NATO forces "dropped munitions that deployed tinfoil-like streamers to drape over power lines and short them out, requiring days to repair."[69] Note that this precaution does not minimize the impact in terms of scope (it still terminated power to civilians), but it does limit it in terms of duration (requiring only days to repair, vice completely destroying it). This is a confluence of Law of War principles: a dual-use object is targetable despite incidental civilian harm when feasible precautions are taken to minimize that harm in accordance with the existing military necessity. Thus, destroying

66 Note, however, that because precautions are tied to reasonableness and feasibility, historical examples, while illustrative, are inherently of limited application. What was reasonable in the days before precision munitions may not be required today. What is feasible today may be more than what was required yesterday. An example of this might be leaflet drops being sufficient in previous conflicts, but mass text message notifications, if technologically feasible, being required in future conflicts as a method of advance warning to civilian populations. In short, this is an inherently evolving standard and so historical examples, while useful, are not necessarily binding.

67 SOLIS, *supra* note 8, at 535.

68 Yoram Dinstein, *Legitimate Military Objectives Under the Current Jus in Bello*, 78 INT'L L. STUD. 139, 156 (2002).

69 SOLIS, *supra* note 8, at 535.

the power stations may have been disproportionate if the military need was only to interrupt power.

Operational Authorities. This step in the analysis is not a Law of War check; it concerns domestic law and authorities. Operational authorities are usually classified, so the discussion will be necessarily general in nature. Considerations in this step of the process will address a wide a variety of control measures. Who is the approval authority for the strike? Does that approval authority include all kinds of munitions or only certain types? Does that authority require any notifications? Is that authority limited by time? Is that authority limited by level of anticipated civilian casualties? Does this strike comply with the rules of engagement in effect at the time? If not a self-defense strike, is the target a declared hostile force—or in the case of cyber or space infrastructure—being used by a declared hostile force? Is a delegation required or permitted, depending on the level one is at? A helpful way to think about operational authorities is by ensuring the decision maker has the authority for that period of time, in that space, for that target, and with that munition.[70]

VI. FRAMEWORK APPLICATION: CYBER CASCADE

The purpose of an analytical framework is to impose discipline and process onto complex problems for consistent solutions. This Part assesses the analytical framework proposed in Part V using the CASCADE scenario from Part III.

A. Does the Law of War Apply?

Whether the Law of War applies turns on whether CASCADE qualifies as a use of force. In this case, CASCADE is designed to disable military ATC systems by erasing all data on the targeted systems, i.e., it is designed to destroy data only. As a direct consequence of that, however, a military unmanned ISR platform is also destroyed. This physical damage is likely foreseeable given the nature of unmanned aerial systems requiring a control connection of some sort and is proximately caused by CASCADE. Accordingly, CASCADE likely constitutes a use of force or an armed attack, meaning the Law of War applies. Because CASCADE is still active in cyberspace and State A relies

70 Because of the operation-specific nature of operational authorities and their generally classified substance, this step of the analytical framework will not be addressed in the application section of this Article. The list of general factors provided here, while not exhaustive, are nearly universal to every operation and will serve the practitioner well in reviewing or planning nearly any operational plan.

on other systems that could be affected by it, CASCADE represents an imminent threat of the continued use of force, entitling State A to use force in self-defense. Furthermore, because CASCADE also targets air defense systems, it reeks of an opening salvo to some larger attack.

B. Distinction

1. State C CASCADE Attack

Even though CASCADE arguably violates article 2(4) of the U.N. Charter's prohibition on the use of force in international politics, as an attack subject to the Law of War it must still comply with the principles of the Law of War. While the focus of this Article is the targeting of cyber and space infrastructure, assessing the CASCADE attack is important for determining an appropriate response in self-defense.

As a weapon, CASCADE is programmed to deploy its payload only on the targeted systems. In many ways this represents the pinnacle of compliance with the goal of distinction. Just as precision guided munitions are not required today but may establish a standard of expected precautions in the attack, so too may cyber weapons that narrowly target precise, discreet military objectives. Whether CASCADE complies with the principle of distinction, however, will depend on the coding of the cyber weapon. For example, it would be important to know whether civilian agencies rely on the same ATC programs and systems that the State A military does in the Johnson Atolls, or whether CASCADE was programmed to target only those specific systems. This determination would drive the intelligence requirements during the target development phase. Alternatively, do State C's command and control capabilities of CASCADE include real time control of where and when CASCADE deploys its payload or is that automated? These are the kinds of issues the legal advisor should raise during the planning process. It bears noting that it took months to deconstruct the Stuxnet attack on which CASCADE is loosely based. So, while the attack may still serve as a *casus belli*, until capabilities are developed to analyze and attribute cyber attacks in near real-time, lawful retaliation likely will not be based on a self-defense rationale as the imminence of the weapon has been neutered by time.

At this juncture, attribution must be addressed. In the scenario, State A was able to rapidly identify the routing of the CASCADE attack, but not necessarily attribute it to a specific

state actor. This is problematic given the interconnectedness of cyberspace. The "unwilling or unable" doctrine is helpful here but remains unsatisfying. Briefly, the unwilling or unable doctrine stands for the prospect that a belligerent state may, consistent with article 51 of the U.N. Charter, use force against hostile armed forces inside of a neutral state's territory when that neutral state is "unwilling or unable to curb the ongoing violation of its neutrality."[71] Sometimes this is referred to as self-help. Its application to terrorists acting from safe haven countries is readily apparent, but, and while little to nothing has been written about it, the doctrine will be difficult to apply to cyberspace operations for the host of questions it inherently raises. Was the neutral state witting? Is the neutral state technically capable of knowing a belligerent routed a cyber weapon through its infrastructure? Do neutral states even have a duty to be aware given the private nature of most cyberspace infrastructure? Given the rate at which data moves, was the neutral state targeted based on an event that took mere seconds? This factor of duration stands in stark contrast to a terrorist cell establishing a base of operations within the neutral country. This issue, while somewhat tangential, is raised merely to highlight the complexity of legal issues associated with attribution. This is likely less complicated in a *jus in bello* context, but if the event is conflict-initiating, as it is in the CASCADE hypothetical, it quickly becomes a technical and intelligence intensive problem.

2. State A Kinetic Response

The data centers and satellite constellations through which CASCADE deployed in search of its targeted systems and which were subsequently attacked by State A were sets of dual-use infrastructure used by both the military and civilian entities. Accordingly, both targets raise the same distinction concerns. State C's military used the data center and the satellite constellation, so these objects satisfy the first part of the test: they make an effective contribution to military action. The second part of the test however, poses a more significant hurdle: does attacking, capturing, or neutralizing the object offer a definite military advantage to the attacker in the circumstances prevailing at the time? This is where State A's kinetic response becomes more questionable. If the destruction of the data center that CASCADE had previously passed through would stop CASCADE from identifying and deploying its payload on future State A targets, then the answer is

71 DOD LAW OF WAR MANUAL, *supra* note 29, §§ 15.2.3.1 n.40, 15.4.2.

easily yes. But if it is unlikely (as it seems) for CASCADE to pass through the data center again, then does it still offer a military advantage? The same doubt applies to the satellite constellation.

Now, before creating nuance where there should not be, it bears noting that "[g]enerally, the reason why the object meets the first part of the definition also satisfies the second part of the definition."[72] Further, "the concept of definite military advantage is broader than simply denying the adversary the benefit of the object's effective contribution to its military operations."[73] This assessment is made in the totality of the circumstances of the overall conflict. For a potential target to be a military object does not require continuous use or even "immediate tactical gains."[74] An example from another domain is helpful here. Take a bridge for example. The destruction of a bridge on a potential line of communication (LOC) in hostile territory may not serve any immediate tactical aim, however, it may serve to isolate enemy forces in a specific region.[75] World War II is replete with examples of lawful bridge destructions throughout Europe despite the fact that those bridges served as both military avenues of approach as well as civilian thoroughfares and even potential civilian evacuation routes.[76] Essentially, these are dual-use objects the denial of which renders a definite military advantage. The data center and satellite constellation in the CASCADE scenario, in many ways, serve as bridges on State C's digital LOC. Cutting that digital LOC denies State C a potential avenue of approach and limits their operations to other access points. Again, the physicality of the cyber and space domain is more determinative than one intuitively assumes.

In this case, both the data center and satellite constellation contributed to States C's use of force, and the destruction of them provides a definite military advantage to State A; consequently, they are lawful military targets. Some scholars may reasonably come to a different conclusion here, likely because the predominant use of the data center is commercial data stor-

---

72 *Id.* § 5.6.5.

73 *Id.*

74 *Id.* § 5.6.7.3.

75 *Id.*

76 MICHAEL BOTHE, KARL JOSEF PARTSCH & WALDEMAR A. SOLF, NEW RULES FOR VICTIMS OF ARMED CONFLICTS: COMMENTARY ON THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949, at 366 (2013) (analyzing the destruction of bridges in anticipation of the Normandy invasion in 1944).

Indeed, some bridges were destroyed purely for the deceptive effect the destruction would have on the enemy. *Id.*

age/transmission. Any weighing of predominant uses though, is an admission that it served at least some military purpose. Furthermore, the weighing and balancing of uses is truly more of a proportionality objection than a distinction objection. The actual use of the data center and satellite constellation make it a dual-use object the destruction of which denies the enemy a digital LOC, and consequently, makes it a lawful military object. That said, all dual-use objects raise a proportionality question because their destruction inherently has a collateral effect, and in terms of cyber and space infrastructure, balancing those factors is going to be even more difficult than the farmer-by-day, insurgent-by-night dilemma of the past twenty years.

C. Proportionality

It is useful to address both Law of War proportionality and self-defense proportionality here, analyzing both the CASCADE strike, and the kinetic response. Often, when a proposed strike initially fails during the planning process for want of appropriate distinction, it is really a proportionality problem, and appropriate feasible precautions can rescope the strike in a way that targets a purely military objective. Finally, unlike in the distinction analysis, the data center strike and the satellite constellation have different effects and thus require separate proportionality analyses.

1. Proportionality of CASCADE Attack

Again, while CASCADE violates the prohibition on the use of force in international politics found in the U.N. Charter and foundational to the rules-based international order, it must still comply with the principle of proportionality because it is a use of force subject to the Law of War. Accordingly, the incidental collateral damage caused by CASCADE must not be clearly excessive when weighed against the definite military advantage to be gained and State C must use reasonable feasible precautions to minimize such collateral damage.

Just as the precision of cyber weapons technologically enables distinction, it can also be used to minimize incidental collateral damage and comply with the proportionality requirements. In this case, CASCADE is designed to only deploy its payload on the targeted systems. The precision of the distinction mechanism enables proportionality, highlighting the interconnectedness of the two principles. As mentioned above, knowing whether and to what extent the targeted systems are also used for civilian ATC

purposes should drive intelligence requirements in the target development phase as that would change the analysis. As drafted, there is no collateral damage in the CASCADE strike, and consequently there is no proportionality concern. A proportionality concern could arise if the CASCADE strike also caused civilian planes to crash—but only if such collateral was foreseeable. There is no proportionality requirement to mitigate the unforeseeable.

2. Self-Defense Proportionality of State A's Kinetic Response

In the CASCADE scenario, State A's kinetic response in self-defense must be proportionate to the CASCADE attack. For force in self-defense to be proportionate does not mean that it has to be of like kind.[77] Self-defense can be a decisive response.[78] If the strikes on the data center and the satellite constellation are calculated (as they appear to be) to terminate the CASCADE operation, and State A is able to correctly identify that State C is the attacker, then the strikes comply with the self-defense requirements of the Law of War. This is particularly the case as CASCADE appears to be actively seeking additional targets. Because the State A strike is narrowly tailored to end the imminent threat from State C, it is proportionate. Here, in self-defense, proportionality does not require a weighing of potential collateral damage. The doctrine of self-defense is about national preservation and the vindication of rights. Accordingly, it is gauging the level of response.[79] Put another way, self-defense doctrines are about national protection—not mitigation of the effect of war, like the Law of War principle of proportionality.

3. Law of War Proportionality of State A's Kinetic Response

State A's kinetic response must also comply with the Law of War principle of proportionality in that the collateral damage caused by its kinetic strike must not be clearly disproportionate to the military advantage gained by the strike.

Beginning with the data center strike, the first step is to clearly identify the potential collateral damage and the potential military advantage to be gained. The strike on the data center destroyed the data center and killed approximately 300 civilian

77 Raffaele Petroni, *The Principles of Self-Defence and Proportionality in International Law: The Case of War Between Israel and Hamas*, CTR. FOR INT'L RELS. & INT'L SEC. (Nov. 13, 2023), https://www.ciris.info/articles/the-principles-of-self-defence/ [https://perma.cc/VR4S-J3V5].

78 *Id.*

79 DOD LAW OF WAR MANUAL, *supra* note 29, § 1.5.1.

employees. The AWS data center predominantly serviced civilian/commercial interests. The military advantages gained by the strike include eliminating that digital LOC to future State C use and cut off any command-and-control connection that it provided to CASCADE.

While the destruction of the data center could cause significant hardship to a variety of civilians and companies depending on the nature of the data stored there, the main collateral damage is the death of 300 civilian employees. Whether that strike on cyber infrastructure is proportionate will depend on the definiteness of the military advantage gained by State A. Here the advantage gained seems speculative, depending on the quantity of other data centers in the region (likely many). If the data center represented State C's only real connection to the internet, then the military advantage gained is quite definite. Similarly, if the data center was the sole connection through which command and control data was flowing, the advantage is even more definite. Whether this is viewed as a violation of the principle of proportionality will largely depend on State A's ability to articulate the definiteness of the advantage gained. Here too, the context matters. Is this the opening salvo of a war, or a singular strike followed by de-escalation? In the scope of wider conflict, this would likely be determined to be a proportionate strike. Especially if State A takes the feasible precautions of striking when the least number of civilians are present or attempting to warn in advance.

Here too a cross-domain comparison is helpful. A strike on a munitions factory conducted at a time to minimize civilian casualties, and which reduces the adversary's ability to produce munitions for the ongoing conflict is usually considered proportionate. While not a perfect comparison because the data center is not creating cyber weapons, the analysis is the same. Another helpful example would be striking a dual-use airport to prevent the deployment of military aircraft despite killing civilian aviation personnel and impacting civilian transportation. Such a strike is proportionate despite the collateral impacts. The data center is a port through which weapons have been deployed and destroying it will definitely reduce the enemy's ability to do so with relatively few casualties.

Turning to the strike on the satellite constellation, the analysis is the same. The anti-satellite missile response destroyed a privately-owned communications satellite constellation consisting of several satellites. The resulting cloud of space debris remained in orbit presenting potential hazards to all other satel-

lites operating in that orbit regardless of category or nationality. The debris cloud will continue to expand over the course of the next several years, continuing to cause collisions and damage to additional space vehicles.

The destruction of the communications satellite gives a military advantage to State A in terms of cutting off a pathway used by State C to deploy and possibly command and control CASCADE. The incidental collateral damage is extensive, long-lasting, and, in many ways, impossible to predict. Not only does it destroy elements of a commercial communications infrastructure used by the general public (a relatively minor inconvenience, likely tolerated by the Law of War), but it also created a cloud of space debris that will go on destroying for potentially years to come. What is uncertain and unforeseeable about it is how much damage it will actually cause.

In 2007, the People's Republic of China conducted an anti-satellite missile (ASAT) test on a non-operational weather satellite that created a cloud of more than 3,000 trackable pieces of space debris expected to remain in orbit for decades.[80] While not conducted during a conflict and not subject to the Law of War, the extensive nature of that incident should inform any assessment of proportionality for space infrastructure proportionality analysis. What remains true is that the collateral damage it may cause is largely speculative, and the Law of War does not require such uncertainty to be accounted for. Further, because there is a lack of customary norms[81] in this domain, it is difficult to assess how the impacts to various orbits should weigh in a proportionality analysis. Finally, while the United States did maneuver a satellite to eliminate a 7% chance of colliding with the space debris and there was significant international outcry over the inci-

---

80 BRIAN WEEDEN, SECURE WORLD FOUND., 2007 CHINESE ANTI-SATELLITE TEST FACT SHEET 1 (2010), https://www.thecipherbrief.com/files/74832/chinese_asat_fact_sheet_updated_2012.pdf [https://perma.cc/GPG3-EDEX].

81 It is worth noting that the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (commonly referred to as the Outer Space Treaty) generally stands for the proposition that outer space should not be militarized and is to be used for peaceful purposes only. *See* Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205. To the extent that state behavior has complied with those provisions since the adoption of the treaty in 1967, such a norm exists. Like much of cyber and space law, however, this assertion remains undeveloped and contested, and is beyond the scope of this Article.

dent, there is little to no information available about any damage actually caused by this ASAT test.[82]

The radioactive fallout from a nuclear weapon provides a *limited* point of comparison when conducting a proportionality analysis on a strike like this because there is a long-term effect that cannot be accurately accounted for prior to the strike. Where the comparison falls apart, however, is in the sheer scope and scale of civilian casualties likely to be caused in the blast of a nuclear weapon, whereas in space there would almost certainly be none.

In short, in this scenario there are no civilian casualties from the State A ASAT strike, which significantly reduces proportionality concerns, even though there is an indeterminable potential for damage to other civilian space infrastructure.

VII. CONCLUSION

As with any dual-use object, targeting cyber and space infrastructure can be lawful as long as it comports with the principles of the Law of War. In one sense, that is about as helpful as saying it is legal so long as it is done lawfully. While that may sound trite, in substance it is actually packed full of factors for planners, commanders, and legal advisors to consider. This Article lays out one method for approaching this problem in the form of an analytical framework based on a hypothetical intended to raise more questions than space allows answers for, but which can serve as a starting point to address the complexities that the next major war will present as customs develop. Because the hypothetical focused the discussion on distinction and proportionality, that is what the framework focuses on. That does not mean the other principles do not apply—they just were not as prominent in this discussion, which is why they are included in the worksheet in Appendix A.

This Article is limited to mere legality—a basic threshold in military operations. It has only barely alluded to prudential wisdom, moral implications, and military efficacy—judgments essential to every military decision—and subjects on which military legal advisors are obligated to advise.[83] Accordingly, a final step in the analyt-

---

82 WEEDEN, *supra* note 80, at 3.

83 *See generally* DEP'T OF THE NAVY, JUDGE ADVOC. GEN. INSTRUCTION 5803.1E, PROFESSIONAL CONDUCT OF ATTORNEYS PRACTICING UNDER THE COGNIZANCE OF AND SUPERVISION OF THE JUDGE ADVOCATE GENERAL (2015) (providing guidance for how attorneys must conduct themselves when practicing law under the supervision of the Judge Advocate General).

Rule 2.1 states in part, "In rendering advice, a lawyer may refer not only to the law but to other considerations such as moral, economic, social, and political factors that may be relevant to the client's situation." MODEL RULES OF PRO. CONDUCT r. 2.1 (A.B.A. 2020); *see* DEP'T OF THE

ical framework beyond the scope of this Article might be: should the target be struck? Once the law in this area is settled, no doubt, the debate will turn to these finer points.

Finally, this Article highlights the degree to which a commander or legal advisor must rely on technical experts and intelligence professionals when making Law of War determinations involving cyber operations—whether planning, executing, or responding to them. This reliance, while perhaps more necessary than in more traditional means and methods of warfare, does not negate the need for either of those professionals to understand the capabilities they are employing. To do so would be to lose oneself in the hubristic feelings of a few ecstatic moments as Lord of the Sky and, like Phaëthon, miss the impending change.

ARMY, ARMY REGUL. 27-26, LEGAL SERVICES: RULES OF PROFESSIONAL CONDUCT FOR LAWYERS r. 2.1 (2018); DEP'T OF THE AIR FORCE, AIR FORCE INSTRUCTION 51-110, PROFESSIONAL RESPONSIBILITY PROGRAM r. 2.1 (2018).

Appendix A: Analytical Framework Worksheet

Law of War Planning Worksheet—Dual Use Focus

	Factors	Notes
Does the Law of War Apply	• The Law of War is a *lex specialis* that applies only to armed conflicts. • Is there an armed conflict? International or non-international? • Does the cyber operation constitute a use of force?	
Military Necessity	• Operation necessary for overall war aims • Does operation create unnecessary death/destruction? • Is the conduct otherwise prohibited by LOAC?	
Distinction	• Is it an inherently military person or object • Is it a military object by its nature, use, location, or purpose	
Proportionality	• Identify collateral effects • Identify military advantages to be gained • Balance • Identify feasible precautions to mitigate potential collateral damage • If dual use: • Is it predominantly military or predominantly civilian? If predominantly civilian, when assessing proportionality, the military interest must be commensurately greater. (I.e., the greater the collateral effects, the greater the military advantage to be gained must be.)	
Humanity	• Identify legitimate military purpose for death/destruction • Is all death/destruction tied to a military objective?	
Honor	• Avoid attempts to skirt LOAC requirements • Avoid undermining protections of LOAC • Perfidy	
Operational Authorities	• Does your commander have the operational authorities in an EXORD or OPORD to conduct the operation? • Do the Rules of Engagement permit the operation • If not, at what level is the approval authority? • Authority at the right time? In the right place? For the right target? For the right weapon?	
Prudential Factors	• Legal, moral, ethical? Economic, social, political factors relevant? • Lawful by awful? • "Headline test" I.e., within the customs and norms?	