NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE DUAL-USE DILEMMA: BALANCING INTERNATIONAL NORMS AND NATIONAL SECURITY

by

Jordan D. Craft

December 2023

Thesis Advisor: Bradley J. Strawser
Co-Advisor: Tristan Volpe

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE THE DUAL-USE DILEMMA: BALANCING INTERNATIONAL NORMS AND NATIONAL SECURITY	**5. FUNDING NUMBERS**
6. AUTHOR(S) Jordan D. Craft	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The distinction between civilian and military assets blurs in an ever-connected world due to an intermingling of dual-use capabilities. Such fusion results in questions regarding the handling, targeting, and leveraging of dual-use assets. Specifically, one asks how the U.S. should redefine a legitimate military objective and adjust U.S. policy in response to the strategic landscape. Traditional wartime roles are eroding and, instead, permitting dual-use technology and dual-use civilians to stress the traditionally held views of just war theory and call into question key aspects of individual culpability beyond that of uniformed combatants. As a result, the U.S. military must address the changing trend of warfare and what is targetable under international law. The law sets a minimum baseline, yet the U.S. needs to identify its moral baseline regarding targeting dual-use capabilities and how that affects national security objectives. The dual-use dilemma is one where international laws and state practices must reflect the reality of non-combatant influence in conflict. Protection for civilians and their assets has, rightly, always been a core tenet of just war. Still, their protection is not absolute. Accountability and culpability need to reflect modern warfare, where ethical fighting aligns with the pursuit of national strategic interests.

14. SUBJECT TERMS dual-use technology, space, cyber, military objective, military target, combatant, distinction, proportionality, law, legal, commercial technology, China, grey-zone	**15. NUMBER OF PAGES** 87
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

THE DUAL-USE DILEMMA: BALANCING INTERNATIONAL NORMS AND NATIONAL SECURITY

Jordan D. Craft
Major, United States Air Force
BS, United States Air Force Academy, 2010
MS, University of Arkansas, 2015

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2023**

Approved by: Bradley J. Strawser
Advisor

Tristan Volpe
Co-Advisor

Carter Malkasian
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The distinction between civilian and military assets blurs in an ever-connected world due to an intermingling of dual-use capabilities. Such fusion results in questions regarding the handling, targeting, and leveraging of dual-use assets. Specifically, one asks how the U.S. should redefine a legitimate military objective and adjust U.S. policy in response to the strategic landscape. Traditional wartime roles are eroding and, instead, permitting dual-use technology and dual-use civilians to stress the traditionally held views of just war theory and call into question key aspects of individual culpability beyond that of uniformed combatants. As a result, the U.S. military must address the changing trend of warfare and what is targetable under international law. The law sets a minimum baseline, yet the U.S. needs to identify its moral baseline regarding targeting dual-use capabilities and how that affects national security objectives. The dual-use dilemma is one where international laws and state practices must reflect the reality of non-combatant influence in conflict. Protection for civilians and their assets has, rightly, always been a core tenet of just war. Still, their protection is not absolute. Accountability and culpability need to reflect modern warfare, where ethical fighting aligns with the pursuit of national strategic interests.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AP-1	Advanced Protocol 1
ASAT	anti-satellite weapon
CCP	Chinese Communist Party
CEO	Chief Executive Officer
CIL	customary international law
DOD	Department of Defense
GPS	global positioning system
ICRC	International Committee of the Red Cross
IHL	international humanitarian law
ISR	intelligence, surveillance, and reconnaissance
JWT	just war theory
LOAC	law of armed conflict
NASA	National Aeronautics and Space Administration
NDS	National Defense Strategy
NSS	National Security Strategy
PLA	People's Liberation Army of China
PRC	People's Republic of China
USSR	Union of Soviet Socialist Republics
WMD	weapons of mass destruction
WWII	World War Two

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The distinction between civilian and military assets continues to blur in an ever-connected world due to an intermingling of dual-use capabilities. Such fusion has led to questions regarding the handling, targeting, and leveraging of dual-use assets and precisely when a trip wire has been crossed from civilian to combatant. Specifically, one asks what the future operating environment will look like regarding dual-use capabilities and how the U.S. should redefine a legitimate military objective and adjust U.S. policy to respond to an ever-changing strategic landscape. Traditionally held just war theory views are stressed regarding dual-use objects, as their usage is no longer constrained to government action. Instead, dual-use assets provide for the ability of commercial actors and civilians to have a grave influence on the battlefield. In addition, this trend creates security dilemmas for the U.S. in the form of detection, attribution, and optics. Dual-use technology presents significant global benefits, yet it is imperative to carefully navigate its inherent risks including international tension, escalation, and the challenges of culpability and non-combatant immunity.

The rapid and deliberate fusion of dual-use technology amongst civilian and military sectors presents a worrisome trend. The distinction between civilian capabilities and their military counterparts continues to blur in an ever-connected world. This dilemma will be increasingly present in conflict worldwide, both in large-scale state-on-state action and operations that fall short of war. No longer is proximity to the battlefield, nor swearing an oath, a pre-requisite for wartime activity and engagement. Unfortunately, modern just war theory views do not account for this civilian transfusion, nor is the U.S. national security apparatus prepared to leverage dual-use technology to its advantage and make informed decisions for long-term security risks.

State governments, and not individuals, have traditionally been held liable for going to war. However, new technologies and capabilities may permit non-state actors, corporations, or even individuals to have power that eclipses that of many governments. Therefore, it is necessary to reevaluate culpability and determine responsibility for wartime and warlike actions. The concept of a legal and lawful combatant needs to be expanded

beyond those in traditional military uniforms to encompass those who play active roles in conflicts, even from remote locations or through technical means.

In addition to reevaluating the ethics and just action of combatants in war, the U.S. military needs to address the changing trend of warfare and what is targetable under international law. Customary international law and international agreements take years to craft and will always be a lagging indicator of right and wrong. Furthermore, the law sets a minimum legal baseline, and the U.S. needs to identify its moral baseline regarding targeting dual-use technology and capabilities. In future conflicts, commanders face questions regarding the legitimacy of attacking dual-use objects. They will require training to prepare for making critical battlefield decisions and identifying the legality and optics of their action. For this reason, the U.S. military needs to incorporate dual-use targets and technology into its exercises and drills to provide commanders lessons learned and insight into the nuance of dual-use targets and objectives in operations that fall short of armed conflict.

The U.S. must also protect itself from vulnerabilities by leveraging dual-use capabilities. Policymakers need to be expressly prescriptive regarding openness to new technologies and how they handle innovation and dissemination of information. The U.S. can achieve a strategic balance in leveraging civilian and militarized dual-use technology by implementing robust safeguards that bolster national security without unduly giving away exquisite technology via the commercial sector.

The dual-use dilemma is not restricted to difficulties facing the United States, but is instead a global dilemma where international laws and norms need to reflect the reality of non-combatant influence in conflict. Protection for civilians and their assets has always been, and should continue to be, one of the core tenets of just war. Still, their protection is not absolute, and current laws and norms offer broad protection and latitude for nefarious action. Accountability and culpability need to reflect modern war, where the power of an individual can significantly influence the battlespace. The principles of just war theory are just as important today, where fighting justly is paramount. War and conflict are not going away; however, the threshold for what constitutes armed conflict is eroding, thus precariously placing the ethics of right and wrong in a difficult position. Dual-use

technology presents significant global benefits, yet it is imperative to carefully navigate its inherent risks, including international tension, escalation, and the challenges of culpability and non-combatant immunity. The international community needs to, as the London Tube reminds us, *mind the gap* regarding dual-use technology, before the doors close and opportunities for peaceful leveraging of dual-use capabilities are irrevocably compromised.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Dual-use technology and civilian-military fusion leveraging technology are far from a new dilemma for the United States. However, the distinction between civilian and military capabilities continues to blur in an ever-connected world. Such fusion has led to questions regarding the handling, targeting, and leveraging of dual-use capabilities and precisely when a trip wire has been crossed from civilian to combatant. The U.S. must continue to leverage dual-use technology to its advantage, conduct operations below the threshold of armed conflict, and make informed decisions for long-term security risks, political farsightedness, and ethical dilemmas. Sarah White, Harvard Ph.D. graduate and U.S. Army cyber officer, notes that as more civilian actors emerge, nation-states must grapple with this balance, both "inside and outside the contours of conflict."[1]

A. PROBLEM STATEMENT AND RESEARCH QUESTION

As these dual-use threats continue to emerge, where "sophisticated dual-use technology is accessible to adversaries in open global markets," an assessment and framework need to be developed to identify when a dual-use capability has crossed a certain threshold and transitioned to a legitimate military objective, targetable under international laws and norms.[2] As a former Senior Economist on the Council of Economic Advisors for the Clinton Administration, Jay Stowsky notes that "the rate of technological diffusion" will accelerate and continually blur the lines on what is a civilian capability compared to a militaristic one.[3] This diffusion is especially apparent in the space and cyber domains as they both present a unique dual-use issue, as "most military equipment now derives from highly sophisticated commercial technology."[4] As a result of this diffusion, there exists a "dead zone" of international cooperation where there is low distinguishability

[1] Sarah White, "Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine" (PhD Diss., Harvard, 2019), 6, https://dash.harvard.edu/handle/1/42013038.

[2] Jay Stowsky, "Secrets to Shield or Share? New Dilemmas for Military R&D Policy in the Digital Age," *Research Policy* 33, no. 2 (March 2004): 257, https://doi.org/10.1016/j.respol.2003.07.002.

[3] Stowsky, 258.

[4] Stowsky, 257.

between civilian and military assets and a high level of integration with its civilian counterparts.[5] This lack of distinction, and an inability to corral the diffusion, presents a significant security threat to the United States and an external advantage to its adversaries. These rivals could leverage ambiguity in their favor, knowing that the U.S. will likely defer any action perceived as an attack on civilians or civilian infrastructure. Understanding that many capabilities exist in this dead zone and that U.S. adversaries relish the unambiguous nature of new capabilities, the problem will only worsen. The U.S. must identify how its military will handle this evolving situation and balance national security with international norms and conditions for targeting dual-use capabilities. Given this increasing diffusion regarding dual-use capabilities, policymakers and military strategists must ask: what will the future operating environment look like regarding dual-use capabilities, and how should the U.S. redefine what a legitimate military objective is and adjust U.S. policy as a response to an ever-changing strategic environment? This thesis explores this question and what possible answers could be on the horizon.

B. BACKGROUND

From the onset, one must define the usage of dual-use technology for shared understanding and baseline. Dual-use, as described in this paper, refers to "goods, software, and technology that can be used for both civilian and military applications."[6] As noted by Vaynman and Volpe, all technology is inherently dual-use, and its capability "shapes the prospects for cooperation in international relations" and influences behavior.[7] The 2022 United States National Security Strategy (NSS) underscores the relationship between civilian and military applications in understanding that "the private sector and open markets have been, and continue to be, a vital source of our national strength and a key

[5] Jane Vaynman and Tristan A. Volpe, "Dual Use Deception: How Technology Shapes Cooperation in International Relations," *International Organization* 77, no. 3 (September 2023): 601, https://doi.org/10.1017/S0020818323000140.

[6] European Commission, "Exporting Dual-Use Items." January 27, 2023, https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en.

[7] Vaynman and Volpe, "Dual Use Deception," 600.

driver of innovation."[8] However, the NSS continues and notes that while the private sector has provided critical strengths for the U.S., it has inversely affected external threats as "emerging technologies transform warfare and pose novel threats to the United States and our allies and partners."[9] The National Defense Strategy (NDS) of the United States acknowledges that "new or fast-evolving technologies and applications are complicating escalation dynamics and creating new challenges for strategic stability."[10] Specifically, the NDS notes that "in the cyber and space domains, the risk of inadvertent escalation is particularly high due to unclear norms of behavior and escalation thresholds, complex domain interactions, and new capabilities."[11] The potential for inadvertent escalation underpins the importance of the U.S. identifying legitimate military objectives in the new era of dual-use diffusion.

Military leaders in Washington understand that, as White notes, the "attributes of cyberspace render it unique among historical military innovations."[12] The unparalleled civil-mil convergence of *both* cyberspace and space "erodes the military's monopoly on both use of force and the underlying technical and professional expertise."[13] Such an erosion yields complications from commercial actors in the field and can influence national policy, capacity, and capability more than ever. However, as mentioned, dual-use capabilities, complications arising from targeting, and international cooperation are not new concepts but ones that the U.S. military needs to deftly manage.

The most cited example of dual-use targeting exists with the U.S. targeting of bearing factories in Germany during the Second World War. Bearings were a "vital component in the tanks, airplanes, machine guns, heavy artillery, and submarines" used by

[8] Joseph Biden, *National Security Strategy of the United States of America* (Washington, DC: White House, 2022), 14, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[9] Biden, 21.

[10] Department of Defense, *National Defense Strategy of The United States of America* (Washington, DC: Department of Defense, 2022), 6, https://apps.dtic.mil/sti/trecms/pdf/AD1183539.pdf.

[11] Department of Defense, 6.

[12] White, "Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine," 5.

[13] White, 6.

the Germans throughout the war.[14] However, such bearings supported the military war effort and were essential for *anything* mechanical, whether military or not. Such a factory could manufacture military bearings one day and civilian applications of a similar nature the following day. In this case, the U.S. military relied on the principle of distinction, codified in the Geneva Conventions, Additional Protocol I (AP-1). AP-1 states that "civilian objects shall not be the object of attack" and that "military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action."[15]

However, two things are worth noting regarding the principle of distinction, as categorized in AP-1. The first is that the United States has not ratified this addendum to the Geneva Conventions, and more apropos for this discussion, that these laws govern the conduct in war. The United States now finds itself in an ethereal state of peace where competitors "seek adverse changes in the status quo using gray zone methods—coercive approaches that may fall below perceived thresholds for U.S. military action."[16] More recent dual-use targeting examples exist in Desert Storm, where U.S. aircraft deliberately targeted Iraqi electrical power facilities.

In Desert Storm, targeting Iraqi electrical facilities had the effect of "crippling Iraq's military command control capability" yet went on to "shut down water purification and sewage treatment plants," resulting in the foreseen hundreds of thousands of civilian casualties due to infectious diseases.[17] While the U.S. justified the attack as a legitimate military target, fulfilling the principles of distinction and proportionality, a RAND study acknowledged that ambiguous situations often exist "where military and civilian assets are

[14] "Ball Bearing," National Museum of American History, accessed February 5, 2023, https://americanhistory.si.edu/collections/search/object/nmah_846532.

[15] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)," U.N.T.S. No. 17512, vol. 1125 § (1977), 256, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977?activeTab=1949GCs-APs-and-commentaries.

[16] Department of Defense, *National Defense Strategy of The United States of America*, 6.

[17] Kenneth R Rizer, "Bombing Dual-Use Targets: Legal, Ethical, and Doctrinal Perspectives," *Air and Space Power Journal*, May 2001, 1, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/Rizer.pdf.

collocated and sometimes difficult to distinguish."[18] The aspect of distinguishability has only become more relevant and, thus, more challenging to diagnose with the advent of action in space and cyberspace.

A lack of distinction is one of two (the other being proportionality) factors significantly affecting a nation's ability to influence, coerce, or cooperate regarding new and emerging technology. Based on distinguishability and the level of integration into civil-military sectors, Vaynman and Volpe offer four zones regarding how technology shapes information constraints on cooperation.[19] Under their principle, a highly distinguishable technology, coupled with low levels of integration (e.g., space from 1957–1970), represents a "permissive zone" where interstate cooperation yields the "best prospects."[20] On the opposite end of the spectrum, the "dead zone" has low levels of distinguishability and high levels of integration (e.g., cyber operations, space operations, biological, and drones), thus generating the worst prospects for interstate cooperation.[21] In addressing dual-use technology, "multilateral treaties and conventions most significantly" impact the control and dissemination of tech.[22] However, in the dead zone, such attempts often "lack adequate implementation and oversight mechanisms to keep up with emerging capabilities."[23]

Furthermore, efforts to protect the development of dual-use technology have not stopped variations of the same fundamental technologies from entering the open global markets, which are leveraged by all nations.[24] For this reason, the dead zone is the assumed starting point in this thesis for identifying and objectifying a legitimate military target in

[18] Matthew Waxman, *International Law and the Politics of Urban Air Operations* (Santa Monica, CA: Rand, 2000), 24, https://doi.org/10.7249/MR1175.

[19] Vaynman and Volpe, "Dual Use Deception," 611.

[20] Vaynman and Volpe, 611.

[21] Jane Vaynman and Tristan Volpe, "Dual Use Deception: How Technology Shapes Cooperation in International Relations" (Working Paper, 2022).

[22] Tara Mahfoud et al., "The Limits of Dual Use," *Issues in Science and Technology* 34, no. 4 (Summer 2018), https://issues.org/the-limits-of-dual-use/.

[23] Mahfoud et al.

[24] Stowsky, "Secrets to Shield or Share?," 266.

strife below the threshold of armed conflict. It is this dead zone where the U.S. finds itself navigating in murky waters, where an adversary matches the United States' ability to leverage dual-use obfuscation. Understanding that this dead zone will prevent international cooperation regarding norms and treaties, the U.S. must identify how it handles military-civilian objectives in a future conflict.

The United States is in an eternal state of grey zone operations "defined by a condition of constant action."[25] New technologies have formed a seamless bridge between civil and military applications. Scholars call for precision in understanding any diffusion between capabilities to develop "tailored risk assessment, governance measures, and opportunities of intervention regarding unintended and unexpected outcomes of emerging technologies."[26] However, the fusion of such technologies has made it desirable for the adversary, as it "can be so readily used outside of a state of armed conflict" and has therefore "contributed to the state of continuous low-level engagements."[27]

The fusion of dual-use technology continues to be a problem that the United States must grapple with, especially concerning whether the state should pursue efforts "domestically, bilaterally, multilaterally—for appropriate restraint, transparency, or control."[28] However, "in a global economy, policies aimed at restricting participation in technology development and keeping the results secret are counterproductive," and it can be assumed that arms export restrictions and control measures will not apply to dual-use capabilities (hence the dead zone).[29] How to act is further complicated when nation-states deliberately join civil and military components together. In the case of China, "Military-Civil Fusion is a national strategy" aimed at returning China to a premier world power with

[25] White, "Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine," 7.

[26] Stefka Schmid, Thea Riebe, and Christian Reuter, "Dual-Use and Trustworthy? A Mixed Methods Analysis of AI Diffusion Between Civilian and Defense R&D," *Science and Engineering Ethics* 28, no. 2 (April 2022): 1–23, https://doi.org/10.1007/s11948-022-00364-7.

[27] White, "Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine," 381.

[28] Christopher F. Chyba, "New Technologies & Strategic Stability," *Daedalus* 149, no. 2 (April 2020): 150, https://doi.org/10.1162/daed_a_01795.

[29] Stowsky, "Secrets to Shield or Share?," 267.

the military to support its aims.[30] China will accomplish this by "acquiring the intellectual property, key research, and technological advances of the world's citizens, researchers, scholars, and private industry."[31] Such fusion is even more complicated when it has the potential to "risk national security" while simultaneously leveraging nefarious methods of acquiring intellectual property.[32]

The United States acted in February of 2023 when such perceived ambiguity made its way to the continental U.S. in the form of a Chinese spy balloon flying at 60,000 feet, right at the upper limit for controlled airspace.[33] The U.S. first publicly acknowledged the balloon when it was over Montana. Eventually, it was shot down by U.S. fighter aircraft once it drifted across the U.S. and into the Atlantic Ocean.[34] Defense Secretary Austin asserts that the balloon was "used by the PRC in an attempt to surveil strategic sites in the continental United States."[35] While this airship was clearly distinguishable as a military asset, future capabilities (e.g., civilian satellites or cyber intrusions) may not be as clear. While the Chinese Ministry of Foreign Affairs issued a statement countering "that the airship is for civilian use and entered the U.S. due to force majeure, which was completely accidental," it was apparent that the airship was not simply a civilian-use balloon.[36] The

[30] Department of State, "The Chinese Communist Party's Military-Civil Fusion Policy," Department of State, accessed February 5, 2023, https://2017-2021.state.gov/military-civil-fusion/.

[31] "The Chinese Communist Party's Military-Civil Fusion Policy," Department of State, accessed February 5, 2023, https://2017-2021.state.gov/military-civil-fusion/.

[32] Department of State.

[33] Jim Garamone, "F-22 Safely Shoots Down Chinese Spy Balloon Off South Carolina Coast," U.S. Department of Defense, February 4, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3288543/f-22-safely-shoots-down-chinese-spy-balloon-off-south-carolina-coast/; Federal Aviation Administration, *Airspace Designations and Reporting Points*, JO 7400.11H (Washington, DC: Federal Aviation Administration, 2023), https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1038054.

[34] Garamone, "F-22 Safely Shoots Down Chinese Spy Balloon Off South Carolina Coast."

[35] Lloyd Austin, "Statement From Secretary of Defense Lloyd J. Austin III," Department of Defense, February 4, 2023, https://www.defense.gov/News/Releases/Release/Article/3288535/statement-from-secretary-of-defense-lloyd-j-austin-iii/#:~:text=The%20balloon%2C%20which%20was%20being,down%20above%20U.S.%20territorial%20waters.

[36] "Statement on the US Claim of Shooting Down the Chinese Unmanned Airship," Ministry of Foreign Affairs of the People's Republic of China, February 5, 2023, https://www.mfa.gov.cn/zyxw/202302/t20230205_11019861.shtml.

statement calls out the U.S. for "obviously overreacting and seriously violating international practice" and says, "China will resolutely safeguard the legitimate rights and interests of relevant companies, while reserving the right to make further necessary reactions."[37] The narrative pushed by China, and action taken by the U.S., exacerbates the complicated reality faced by dual-use capabilities and the necessity for the U.S. policymakers and implementers to carefully assess the situation from the viewpoint of strategic security coupled with international norms and ethics for the civilian application of technology.

C. THESIS STRUCTURE

This research will be conducted by leveraging historical case studies and application to present-day issues affecting the dual-use dilemma. An analysis will be undertaken via contrasting lenses: Just War Tradition (JWT) (ethical) and international humanitarian law (IHL) (legal) with security and stability within the United States (strategy). By illuminating the nuances between JWT/IHL and domestic strategy, a comprehensive understanding of the evolving dual-use landscape will emerge, seeking, at the very least, to identify shortcomings and issues regarding the status quo of how the U.S. handles dual-use technology.

Customary international law and norms governing military objectives were outlined and written for a war waged decades ago. However, the gap between civilian and military combatants and assets has continued to blur, resulting in ambiguity. The "digitization of societies" has "fundamentally shifted the role of civilian involvement in conflicts both in both quality and quantity."[38] As a result, a gap exists that fails to identify and define a military objective in an ever-changing dual-use landscape. This thesis will seek to identify that gap, what led to the gap, and provide an insight into defining a military objective in grey zone conflict.

[37] "Statement on the US Claim of Shooting Down the Chinese Unmanned Airship."

[38] Kubo Mačák and Mauro Vignati, "Civilianization of Digital Operations: A Risky Trend," *Lawfare*, April 5, 2023, https://www.lawfaremedia.org/article/civilianization-digital-operations-risky-trend.

II. JUST WAR THEORY AND INTERNATIONAL HUMANITARIAN LAW

The convergence of the principles contained within modern Just War Theory (JWT) and dual-use capabilities rapidly become an issue in modern ethics as dual-use capabilities blur the line between civilian and military objectives. This convergence calls into question the definition of a legitimate military objective. While international agreements, customary international law (CIL), and international humanitarian law (IHL) attempt to shed light on such issues, all parties seek to take advantage of legal ambiguity and "create and maintain an asymmetrical legal environment that favors their own operations and disadvantages" their adversary.[39] However, JWT principles offer a higher level of illumination, not bound by laws, borders, or treaties, as it addresses the justification for going to war and conduct in war.

Grounded originally in religion, honor, or chivalry, most cultures have some idea of restraint in war and that universal humanitarian values govern such conduct in war.[40] Stemming from the Western tradition of St. Augustine and later St. Thomas, modern just war theory has departed from wholly religious accommodations and beliefs to more secular ones, having been blended along the way to what is now an amorphous set of "articulated norms, customs, professional codes, legal precepts, religious and philosophical principles, and reciprocal arrangements."[41] However, a generally accepted set of criteria exists for entering conflict and expected conduct therein. In traditional JWT, scholars assess the morality of war through two lenses: *jus ad bellum,* which addresses the decision to go to war, and *jus in bello*, just conduct in war. A third emerging assessment, *jus post bellum,*

[39] Aurel Sari, "Hybrid Warfare, Law, and the Fulda Gap," in *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, ed. Christopher Ford and Winston Williams (New York: Oxford University Press, 2018), 164.

[40] Daniel Muñoz-Rojas and Jean-Jacques Frésard, "The Roots of Behaviour in War: Understanding and Preventing IHL Violations," *International Review of the Red Cross* 86, no. 853 (March 2004): 189–206, https://doi.org/10.1017/S1560775500180150.

[41] Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: Basic Books, 2006), 44.

addresses morality during the termination phase of a conflict.[42] Such considerations are outside the scope of this thesis, however.

Waging armed conflict against another human represents one of the gravest attacks an individual and nation can initiate. As such, the decision to go to war demands the highest levels of scrutiny. Therefore, "war shouldn't be entered into lightly, flippantly, or without serious consideration."[43] In deciding the morality of conducting a war, the initiator must meet several *jus ad bellum* criteria, including a just cause with just intent, waged by a legitimate authority, a public declaration, proportionality, last resort, and a reasonable chance of success.[44]

A. *JUS AD BELLUM* TENANTS

The foundation for *jus ad bellum*, just cause, dictates that going to war for an unjust cause is immoral.[45] Definitions of what constitutes just cause have evolved over the years. However, Thomas Aquinas initially said, "Those who are attacked, should be attacked because they deserve it on account of some fault."[46] Aquinas explains that those faults include avenging wrongs and restoring what one has "seized unjustly."[47] Following the Treaty of Westphalia in 1648, states began to define just causes as those required "for defense of the state."[48] The United Nations Charter, signed in 1945, codified limitations on using force in two circumstances, self-defense of a victim state and self-defense of another state, when approved by the Security Council "to maintain or restore international

[42] Brian Orend, "Jus Post Bellum: The Perspective of a Just-War Theorist," *Leiden Journal of International Law* 20, no. 3 (September 2007): 571, https://doi.org/10.1017/S0922156507004268.

[43] Matthew Hallgarth, "Just War Theory and Remote Military Technology: A Primer," in *Killing By Remote Control*, ed. Bradley Strawser (New York: Oxford University Press, 2013), 30.

[44] Hallgarth, 31.

[45] Jeff McMahan, "Just Cause for War," *Ethics & International Affairs* 19, no. 3 (December 2005): 1, https://doi.org/10.1111/j.1747-7093.2005.tb00551.x.

[46] Thomas Aquinas, *Summa Theologica, Part II-II*, trans. Fathers of the English Dominican Province (Salt Lake City, Utah: Project Gutenberg, 2006), https://www.gutenberg.org/ebooks/18755.

[47] Aquinas.

[48] Martin Cook, "The Role of the Military in the Decision to Use Armed Force," in *The Ashgate Research Companion to Military Ethics*, ed. James Johnson and Eric Patterson (New York: Routledge, 2016), 50.

peace and security."[49] Over the last several decades, numerous countries and agencies have attempted to expand the conditions for just cause to include collective self-defense, responsibility to protect, and punishing others for "grievous rights violations."[50] In addition to having a just cause for war, one must also wage it with just intent. Inextricably linked to just cause, yet nuanced, just intent ensures that wars are "fought with the right motives…to right an injustice and then to restore peace."[51]

A competent and legitimate authority must wage war for a war to be just. War is not "the business of a private individual" or organization, but rather by legitimate governing authorities such as recognized governments or the United Nations Security Council.[52] For the United States, the Constitution is explicitly clear that it is the purview of Congress to declare war, yet expanding executive powers have initiated military action of their own accord for decades.[53] Waging war by a legitimate authority for a just cause needs to be publicly declared for it to be morally justified. A credible declaration of war provides intent and offers the adversary one last attempt to compel to avoid armed conflict.

Proportionality is a factor in just war theory, both in *jus ad bellum* and *jus in bello* narratives. For *jus ad bellum,* the anticipated strategic benefits of the war must outweigh the expected harms and costs associated with the conflict, considering both military and civilian costs on the instigator and adversary relative to the political aim or objective (*raison d'etat*). This tenant of JWT ensures that "trivial injustices" do not lead to conflict.[54]

Considering war's destructive nature, competent authorities should pursue it only after exhausting all peaceful means of conflict resolution or when they are unavailable. While peaceful means do not necessarily mean painless, they seek to obtain the desired objective via diplomatic, economic, or other means short of military action. However, such

[49] United Nations, "Charter of the United Nations and Statute of the International Court of Justice" (1945), 9, https://treaties.un.org/doc/Publication/CTC/uncharter-all-lang.pdf.

[50] Hallgarth, "Just War Theory and Remote Military Technology: A Primer," 30.

[51] Hallgarth, 31.

[52] Aquinas, *Summa Theologica, Part II-II*.

[53] *U.S. Constitution, Art. 1, Sec. 8, Cl. 11*.

[54] Hallgarth, "Just War Theory and Remote Military Technology: A Primer," 31.

aforementioned actions generally take time to yield the desired behavior and call into question when the legitimate last resort has been exhausted.

Lastly, one should only wage war if there is a reasonable chance of success. When initiated without a chance of achieving the stated objectives, the suffering and costs associated with a conflict will have been in vain and unjust. However, assessing the probability of success is not always straightforward, allowing for a David versus Goliath (or Vietnam versus the United States) opponent to prevail.

B. CHALLENGES WITH DUAL-USE CAPABILITIES AND *JUS AD BELLUM*

While most dilemmas regarding the changing nature of dual-use capabilities affect the *jus in bello* domain, analyzing the nuances of *jus ad bellum* provides insight, especially regarding discussions of legitimate authority and public declaration. For just cause and just intent considerations, states need to be weary of dual-use capabilities, real or perceived, as such buildup could provide just cause for an adversarial attack. For example, if a state uses its dual-use capable chemical or biotech program to weaponize agents, it could satisfy the principles of just cause for a preemptive attack. However, as discussed in subsequent sections, the differentiation of a biological weapon program from legitimate research and development is difficult to ascertain.[55] From a historical perspective, when the U.S. coalition attempted to reduce Iraq's weapons of mass destruction capabilities, the U.S. military conducted Operation Desert Fox, which deliberately targeted "dual-use facilities potentially related to WMD production and storage."[56] More recently, in the ongoing conflict with Russia and Ukraine, the bombing of the bridge that connects Crimea to mainland Russia was the source of contentious dialogue between President Zelensky and

[55] W. Seth Carus, "A Century of Biological-Weapons Programs (1915–2015): Reviewing the Evidence," *The Nonproliferation Review* 24, no. 1–2 (January 2017): 130, https://doi.org/10.1080/10736700.2017.1385765.

[56] Daniel Brunstetter, "The Decision to Use Military Force in Recent Moral Argument," in *The Ashgate Research Companion to Military Ethics*, ed. James Johnson and Eric Patterson (New York: Routledge, 2015), 30.

President Putin regarding the legitimacy of dual-use targeting.[57] History reflects that while numerous dual-use capabilities are considered legitimate military objectives, their ability to influence a war may permit a just cause establishment.

One of the main *jus ad bellum* domains affected by dual-use technology are the principles of legitimate authority and public declaration. Whereas in past wars, where presidents and parliaments declared war, future conflict will be waged not just by nation-states but by non-state actors and individuals who "will be able to target military forces and civilian infrastructure."[58] The ability of non-state actor groups (e.g., Al-Qaida, Hezbollah, and even the Red Cross) has often influenced world politics and conflict. However, the emergence of pure civilian action in support of an objective or claim is unprecedented. When Elon Musk, the CEO of Space-X, provided fighters in Ukraine with access to his network of Starlink satellites, he injected himself into a conflict unbound by the typical laws of war. However, such undue influence on the war effort is subject to continual support. Musk acknowledges that "we are not in a position [to] fund the existing terminals for an indefinite period of time."[59] Removing a critical communications node the Ukrainians have come to rely on will deal a significant blow to wartime capability.

While the civilian support of Musk to the war effort was overt, individual influence and action on war face a much darker picture regarding attribution due to cyber activity. Most exquisite cyber attacks (e.g., Stuxnet) stem from established nations with robust cyber capabilities; the threshold for cyber influence has lowered, thus permitting significant action and influence at the individual level. For example, in 2008, a teenager injured twelve when he leveraged a homemade transmitter to trip rail switches and reroute trains off their tracks or, in 2015, individual hackers leveraged phishing emails to gain credentials to a German steel mill and conducted an uncontrolled shutdown of the control system resulting

[57] Euractiv, "Crimea Bridge Is Legitimate Military Target, Zelenskyy Says," Euractiv, July 22, 2023, https://www.euractiv.com/section/global-europe/news/crimea-bridge-is-legitimate-military-target-zelenskyy-says/.

[58] U.S. Army Training and Doctrine Command, *The Operational Environment and the Changing Character of Warfare* (Fort Eustis, VA: Department of the Army, 2019), 23.

[59] Alex Marquardt, "Exclusive: Musk's SpaceX Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick up the Tab," *CNN*, October 14, 2022, https://www.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.

in a damage of millions of dollars.[60] A legitimate authority did not sanction such actions and represents a hazardous outlook on individuals' capability to leverage a digital use of force to confer physical damage to persons and property.

Similarly, covert cyber action is often waged without a formal declaration and instead conducted without attribution or identification. While there are many theories on who conducted the Stuxnet attack, no nation-state, non-state actor, nor individual has credibly claimed responsibility for the assault.[61] However, even if an individual or non-state actor claims the attack, questions arise whether the attack may also be attributed to the state.[62] Given that states wage conflict, not individuals, problems arise regarding whether the attack falls under "state responsibility so to trigger the application of the *jus ad bellum* rules."[63] Given the changing nature of conflict, this raises the question, should individuals, not just states, be held liable for the just war theory framework of *jus ad bellum* assessments?

Given the previous example of Elon Musk providing communications connectivity that has proven to be "an integral part of the Ukrainian army's kill chain," a *jus ad bellum* proportionality argument shall be assessed regarding whether a Russian attack on those satellites would be globally proportionate. Russia is already engaged in an unjust war with Ukraine, and by attacking a satellite network owned by an American company, they could be initiating American involvement in the war, thus greatly extending the magnitude of the conflict. It is unlikely, although not a zero percent chance, that Russia would not seek state-on-state conflict with the United States over Ukraine or, more prescriptively, over the

[60] "6 Cyber Attacks That Caused Property Damage," The ALS Group, March 14, 2017, https://info.thealsgroup.com/blog/cyber-attacks-property-damage.

[61] Andrew Foltz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate," *Joint Forces Quarterly* 4th Quarter, no. 67 (2012): 44, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf.

[62] Stuxnet is believed to have been developed as a joint operation between U.S. and Israeli intelligence services, however no official claims have been made for the attack. Council on Foreign Relations, "Stuxnet" (New York: Council on Foreign Relations, July 2010), https://www.cfr.org/cyber-operations/stuxnet.

[63] Marco Roscini, "World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force," in *Max Planck Yearbook of United Nations Law*, ed. Armin von Bogdandy and Rudiger Wolfrum, vol. 14 (Leiden, NL: Brill, 2010), 97, https://brill.com/view/journals/mpyo/14/1/article-p85_4.xml.

attacks on a capability supporting Ukraine. Such an action would not be globally proportionate relative to their objectives. Furthermore, the international community will unlikely perceive this action as globally proportionate relative to their unjust war aims.

Continuing the theme of an attack on the Starlink satellite network, a deliberate attack on the civilian-owned network is permittable under the auspices of *jus ad bellum* principle of last resort when "all other available means have failed or are likely to fail."[64] In this scenario, when attacking a delicate dual-use capability that will affect its civilian counterpart, extreme prudence needs to occur and ensure that all other aspects of mediation have been exhausted. This is a high bar for dual-use capability, and "all other available means" is a nebulous standard to uphold, thereby proving challenging to satisfy this requirement.[65]

Lastly, a state may engage in conflict and target a dual-use capability when reasonably achieving its stated objectives. However, an accurate assessment shall be undertaken to comprehend the actual capabilities and limitations of the objective in question. A dual-use capability is unlikely to be an adversary's true center of gravity. As Augustine notes, "war is waged in order that peace may be obtained," any action against a dual-use objective must be reasonably assured that doing so will further the cause for a conclusion to the conflict.[66]

In summary, the principles of *jus ad bellum* include a just cause with just intent, waged by a legitimate authority, a public declaration, proportionality, last resort, and a reasonable chance of success. However, hesitation exists regarding the morality of engaging and targeting any dual-use capabilities, given the nuances and high bars set therein. These principles are but one set of moral recommendations for going to war; the other, *just in bello*, analyzes proper conduct while engaged in a conflict.

[64] Roscini, 119.

[65] Roscini, 119.

[66] St. Augustine, "Letter 189," New Advent, 418AD, https://www.newadvent.org/fathers/1102189.htm.

C. *JUS IN BELLO* TENANTS

While both *jus ad bellum* and *jus in bello* tenants are rooted in traditional Just War Theory principles outlined by St. Augustine and St. Aquinas, *jus in bello* finds itself in modern nomenclature in ways that *just ad bellum* is not. *Jus in bello* principles were adopted by modern treaties, customs, and practices and can also be termed international human law (IHL). IHL focuses on the humanitarian aspect of conflict, where it seeks "to limit the suffering caused."[67] This focus on conduct within war bypasses the *jus ad bellum* argument and applies *jus in bello* "irrespective of the reasons for the conflict."[68] Walzer identifies this difference "between the war itself, for which soldiers are not responsible, and the conduct of the war, for which they are responsible."[69] For this reason, it is possible to satisfy the requirements of one category and not the other.

Whereas *jus ad bellum* has numerous principles to satisfy for a war to be morally justified, *jus in bello*, or the right conduct in war, predominantly focuses on proportionality and distinction/discrimination.[70] An interconnectedness between these two tenants as states need to ensure that "particular military missions be reasonably assessed as militarily necessary to achieve justified goals of the conflict."[71] In this light, actions in conflict shall only be undertaken to further the goals and objectives of fulfilling the reasons for the conflict in the first place.

With regard to proportionality, unlike *jus ad bellum* proportionality, where the anticipated benefits of the war must outweigh the expected harms and costs associated with the conflict on a strategic scale, *jus in bello* proportionality asserts that a "military objective may be attacked only after an assessment leading to the conclusion that civilian losses are

[67] "Jus Ad Bellum and Jus in Bello," Internantional Committee of the Red Cross, October 29, 2010, https://www.icrc.org/en/document/jus-ad-bellum-jus-in-bello.

[68] International Committee of the Red Cross, *International Humanitarian Law: Answers to Your Questions* (Geneva: International Committee of the Red Cross, 2023), 9, https://shop.icrc.org/international-humanitarian-law-answers-to-your-questions-pdf-en.html.

[69] Walzer, *Just and Unjust Wars*, 38.

[70] Alexander Moseley, "Just War Theory," Internet Encyclopedia of Philosophy at the University of Tennessee at Martin, accessed November 21, 2023, https://iep.utm.edu/justwar/.

[71] Hallgarth, "Just War Theory and Remote Military Technology: A Primer," 31.

not expected to outweigh the military advantage foreseen."[72] In other words, certain precautions and avoidances shall be taken during a conflict to ensure minimal loss of civilian life, infrastructure, or objects.

In adherence to the law, the principle of proportionality is rooted primarily in Additional Protocol I of the Geneva Conventions (AP-1), articles 51 and 57. However, it is essential to address two critical underpinnings of AP-1. The first is that the protocol is scoped to provide guidance during "international armed conflicts" and that, in theory, the persistent low-level engagement of state actors and non-state actors alike rise to neither the threshold of "armed" nor conflict.[73] Furthermore, the United States is a signatory to AP-1, yet they have not ratified the treaty.[74] While being a signatory exemplifies support for AP-1, the lack of ratification means the treaty does not legally bind the State.[75] Nonetheless, even though the U.S. has not ratified AP-1, the principle of proportionality under IHL is understood to constitute customary international law and, as such, exists independent of treaties.[76]

Specific to AP-1, Article 51 governs the protection of the civilian population, and Article 51(5)(b) notes that indiscriminate attacks are those that "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[77] AP-1 goes on to note in Article 57 that concerning

[72] International Committee of the Red Cross, *International Humanitarian Law: Answers to Your Questions*, 47.

[73] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 279.

[74] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I).

[75] Of Note: China has signed and ratified AP-1, Russia withdrew their ratification in 2019, and Iran and Pakistan have signed but not ratified AP-1. Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I).

[76] Anaïs Maroonian, "Proportionality in International Humanitarian Law: A Principle and a Rule," *Lieber Institute West Point*, October 24, 2022, https://lieber.westpoint.edu/proportionality-international-humanitarian-law-principle-rule/.

[77] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 267.

proportionality, attacks "shall be canceled" if they were to cause incidental civilian harm or damage.[78] While proportionality addresses the balance between civilian harm and military advantage, discrimination addresses the distinct difference between civilian and military objectives.

The principle of distinction in *jus in bello* forbids direct and deliberate attacks on civilians and civilian-use objects.[79] The previously mentioned AP-1, codified under customary international law, states in Article 48, "the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives."[80] The International Committee of the Red Cross notes that for civilians to be targeted, they must have "directly participated in hostilities."[81] Although seemingly straightforward on the left and right bounds, the principles of proportionality and distinction often contradict military strategy and objectives.

During the firebombing raids on Tokyo in 1945, U.S. forces conducted *Operation Meetinghouse*, where 300 B-29 Superfortresses reigned incendiary fire upon Tokyo, yielding more deaths than either of the atomic bombs dropped in Japan or the Dresden fire raids.[82] These bombing campaigns targeted civilian areas indiscriminately, resulting in

[78] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 269.

[79] William Vincent O'Brien, *The Conduct of Just and Limited War* (New York, N.Y: Praeger, 1981), 37.

[80] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 264.

[81] International Committee of the Red Cross, *International Humanitarian Law: Answers to Your Questions.* The ICRC states: "A party to an armed conflict may direct an attack only against combatants or military objectives. Neither the civilian population nor individual civilians may be attacked unless and for such time as they directly participate in hostilities (see box). Attacks must be strictly limited to military objectives and may not be directed against civilian objects. In so far as objects are concerned, military objectives are limited to those objects that by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage. Typical military objectives are establishments, buildings and positions where enemy combatants, and their matériel and armaments, are located, and military means of transportation and communication. When civilian objects are used for military purposes (e.g. a civilian train that is used to transport weapons and combatants) they may be regarded as military objectives."

[82] Tom Demerly, "The Aviationist: 73 Years Ago Today: The Deadliest Air Raid in History, Operation Meetinghouse.," Newstex, March 9, 2018, https://www.proquest.com/docview/2012144060/citation/A8DF2CFD58284FBDPQ/1.

unimaginable harm to civilians and damage to their infrastructure. Moreover, such wide-area bombing raids were widely "disproportionate to their contribution to the war effort, either in political or military terms."[83] The massive scale of these attacks, with the known and deliberate targeting of civilian areas, is unquestionably a dark stain on the *jus in bello* adherence by the United States. In recounting their actions, Robert McNamara, former U.S. Secretary of Defense, acknowledged that the U.S. was "behaving as war criminals. LeMay recognized that what he was doing would be thought immoral if his side had lost. But what makes it immoral if you lose and not immoral if you win?"[84] Winning or losing has no bearing on ethics, and post WWII, conventions, treaties, and protocols established left and right bounds for such indiscriminate and disproportionate behavior.

While WWII saw numerous instances of what today would be considered war crimes, rapid technological advancements and adherence to international and just war norms have yielded numerous examples of strategic strikes. What would have taken dozens of aircraft to accomplish in WWII can be accomplished today with one or two targeted munitions. Recent advancements in aerial superiority and precision weaponeering have permitted military attacks without damaging the surrounding area and minimizing harm to the civilian population. This prescriptive capability was reflected in a 2006 urban airstrike in Baghdad on al-Qaeda leader Abu Musab al-Zarqawi. The attack represents the technological, intelligence, and rule of law maturation that has happened over the last few decades, as it was done with a single munition with minimal yield and adverse effects.[85] The surgical strike adhered to the principles of distinction and proportionality while still achieving the military objective.

D. CHALLENGES WITH DUAL-USE CAPABILITIES AND *JUS IN BELLO*

While new weapons targeting technology and increased intelligence, surveillance, and reconnaissance (ISR) capabilities have ensured military leaders are more prescriptive

[83] O'Brien, *The Conduct of Just and Limited War*, 339.

[84] *The Fog of War,* directed by Errol Morris (2003; Los Angeles, CA: Sony Pictures Classics, 2003), https://tv.apple.com/us/movie/the-fog-of-war/umc.cmc.3j815y9s5id2nvfztrlfh75il.

[85] "Abu Musab Al-Zarqaw Dead," U.S. Department of Defense, 2006, https://www.defense.gov/Multimedia/Photos/igphoto/2001967287/.

in their proportionality decisions, the civil-military diffusion has resulted in numerous capabilities leveraged simultaneously by civilian and militant actors. This simultaneous use of assets yields complications in the *jus in bello* realm concerning the proportionality of an attack and distinguishing between civilian and military use cases. As modern just war theory evolved alongside international law, neither could have predicted nor accounted for the increasing fusion between military and civilian capabilities. Two case studies, one fictional and one actual, will be applied to highlight and identify challenges associated with the principles of proportionality and distinction in modern warfare.

1. Case Study 1: Proportionality

Scenario: Fractured country "A," Aggressistan, is waging a war of aggression within the borders of Country "B," Benevolentia. Benevolentia enjoys worldwide support in repelling Aggressistan, and as a result, Aggressistan is becoming desperate to obtain an asymmetric advantage on the battlefield. Aggressistan has acquired exquisite means to conduct attacks on the worldwide GPS constellation, rendering the network inoperative for "X" time. Would such an attack be proportional under IHL?

In an era where all technology is dual-use to some degree, a prescriptive approach needs to be identified as to when a trip wire has occurred concerning proportionally targeting a dual-use system. The above scenario reflects an example that is classically and inherently dual-use. Three questions, among countless others, need to be addressed regarding the proportionality of such an attack: What constitutes an attack? Is it a legitimate military target? Is it proportional?

a. What constitutes an attack?

The world finds itself in a perennial grey zone of armed conflict, where the very definition of what constitutes an attack under the principles of LOAC is in question. AP1, Article 49 designates an attack as "acts of violence against the adversary, whether in offence or in defense."[86] Article 49 further notes that the provisions contained therein

[86] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 264.

apply to "any land, air or sea warfare which may affect the civilian population, individual civilians or civilian objects on land."[87] Although not explicitly stated, it shall be reasonably expected that the provisions carry forward to all domains, including space and cyber, if they meet the required threshold for attack. The U.S. Law of War Manual supports this claim by asserting that "law of war treaties and customary law of war are understood to regulate the conduct of hostilities, regardless of where they are conducted."[88]

Furthermore, while conventional wisdom has viewed an attack as something that was achieved through physical force, similar results are now able to be achieved through non-physical and non-kinetic means. The *Tallinn Manual* attempts to connect the two seemingly unconnected realms of conduct under LOAC and previously excluded cyber capabilities. The *Tallinn Manual* asserts that "acts of violence should not be understood as limited to activities that release kinetic force," but rather, "the crux of the notion lies in the effects that are caused."[89] This refined narrative thereby focuses not on how an act of violence occurred, but on what effect the act had…were there "violent consequences?"[90] If these violent consequences result in "damage, destruction, injury, or death," then they would qualify as an attack under LOAC and, therefore, are subject to the principles of proportionality and distinction.[91] For this reason, while the above scenario did not specify whether the attack was kinetic (via an anti-satellite (ASAT) missile, on-orbit attack, or otherwise), it is largely irrelevant as the effects caused would be largely the same, but with key differences being scalability and reversibility. These differences will be discussed later in addressing the proportionality question. In any case, an attack aimed at disrupting the GPS satellite network will undoubtedly result in violent consequences for both the civilian and military populations.

[87] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 264.

[88] Department of Defense, *Law of War Manual* (Washington, DC: Department of Defense, 2023), 983, https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF.

[89] Michael Schmitt and Liis Vihul, eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second edition (Cambridge: Cambridge University Press, 2017), 415.

[90] Schmitt and Vihul, 415.

[91] Schmitt and Vihul, 416.

b. Is it a legitimate military target?

Given that an attack on a satellite network, via kinetic or non-kinetic means, *can* constitute an attack under LOAC, the next question to answer is whether the GPS constellation is a legitimate military target. The military usage for the GPS network is extensive, relying on its usage for precision weapons, navigation, and timing in all domains. Given its "nature, location, purpose, or use," GPS is undoubtedly a military objective.[92] However, like many other space-based assets, GPS is critical to not only military infrastructure, but civilian as well. In a 2011 economic impact report, the European Commission concluded that "6–7% of GDP in Western countries" relies on satellite navigation, including GPS and the European Galileo network.[93] This number has undoubtedly increased over the last decade.

Due to this reliance, arguments have been made that under Article 54 of AP-1, GPS is a protected entity and, therefore, disqualified as a legitimate military target as it is "indispensable to the survival of the civilian population."[94] However, AP1 explains that areas deemed indispensable include "foodstuffs, crops, livestock, drinking water" that would deny a population sustenance.[95] While GPS is used heavily in agriculture, and its outage could result in damages exceeding $1B per day, the U.S. Law of War Manual holds that economic harm is not a factor when considering the legitimacy of a military objective.[96] For these reasons, this burden is unlikely to meet the threshold laid out in AP-1, and the GPS constellation may be deemed a legitimate military target.

---

[92] Jack Beard, "The Principle of Proportionality in an Era of High Technology," in *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, ed. Christopher Ford and Winston Williams (New York, NY: Oxford University Press, 2019), 284.

[93] European Commission, "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Mid-Term Review of the European Satellite Radio Navigation Programmes" (Brussels: European Commission, 2011), 2, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0005:FIN:EN:PDF.

[94] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 267.

[95] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 267.

[96] Michael Gallaher, "Economic Benefits of the Global Positioning System," https://www.gps.gov/governance/advisory/meetings/2019-11/gallaher.pdf; Department of Defense, *Law of War Manual*, 270.

c. Is it proportional?

Having established that attacking the GPS satellite network, via kinetic or non-kinetic means, constitutes an attack under IHL and that it is indeed a legitimate military target, an assessment shall be made governing the proportionality of the attack. As noted from the previous section, proportionality under the *jus in bello* tenant of war holds that an attack is proportionate if, among other things, the means and outcome are balanced in "relation to the concrete and direct military advantage anticipated," and that civilian losses are not expected to outweigh the military advantage.[97]

The scenario was vague regarding the method and vector of attack, leaving the possibility of a wide range of attacks stemming from kinetic ASAT attacks to non-kinetic cyber disruption. Should *Aggressistan* go with the kinetic option of an ASAT attack or similar, not only will the attack degrade and deny GPS usage for the military and civilian users (an extreme burden), but it could also artificially induce what is called the "Kessler Effect," wherein satellite debris from a kinetic explosion increases the probability of further collisions, "leading to the growth of a belt of debris around the earth."[98] This debris field could render an entire portion of the medium earth orbit (the path in which GPS satellites orbit) unusable by all satellites, thereby amplifying the downstream and expected effects caused by a kinetic attack on the GPS satellite network. For this reason, such a kinetic attack will likely be seen as indiscriminate under IHL as it fails the principle of proportionality.

While a kinetic ASAT attack can be seen as unproportional as it is neither scalable nor reversible, a cyber-attack may avert these concerns. A cyber-attack is unlikely to cause a Kessler-style debris field (unless the attack is aimed at de-orbiting a satellite and forcing a collision with another) and is, instead, more likely to cause disruptive events. As stated earlier, an attack on the GPS network will adversely affect the civilian population.

[97] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 269.

[98] Donald J. Kessler and Burton G. Cour-Palais, "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt," *Journal of Geophysical Research: Space Physics* 83, no. A6 (June 1978): 2637, https://doi.org/10.1029/JA083iA06p02637.

However, the U.S. Law of War Manual asserts that "mere inconveniences or temporary disruptions to civilian life need not be considered" in proportionality assessments.[99] A kinetic attack on the network could be expected to down the GPS network for quite some time, yet a cyber-attack could be more prescriptive, attacking specific GPS frequencies for specific locations and durations. This prescriptive approach would allow a cyber-attack to be more discrete, affecting only the military objective while mitigating any foreseen civilian harm and, therefore, satisfying a proportionality requirement in IHL.

The closing gap between pure military capabilities and technologies compared to their civilian counterparts will affect how wars are fought. In the above case study, *Aggressistan* sought to degrade or destroy the global positioning satellite network. As the GPS network is inherently dual-use, it is easily understood to be seen as a legitimate military objective. However, destroying the system would have grand consequences, expanding far beyond the scope of any conflict between *Aggressistan* and *Benevolentia*. While this is an extreme example, the confluence of capabilities will continue to further proportionality debates amongst the IHL community. However, the above example was inherently a dual-use capability, further questions arise when the line between civilian and military is not as clear, when there is no distinction, or when capabilities can flow simultaneously between being a military asset and a civilian one.

2. Case Study 2: Distinction

Scenario: The war in Ukraine has resulted from unwarranted aggression from a global power not seen since the onset of WW2. Future conflicts were believed to have removed civilians from the battlefields, but the ongoing war has only seemed to bring them closer to the frontline. After being identified and asked by the Ukrainian Defense Forces, the hero "Drone Boy" of Ukraine, Andrii Pokrasa, helped the Ukrainian Army by flying his personal drone over the battlefield, identifying advancing Russian troops, and passing coordinates on to friendly forces.[100] *These coordinates were then passed to Ukrainian*

[99] Department of Defense, *Law of War Manual*, 269.

[100] Michela Moscufo, "'Drone Boy' Becomes Hero in Ukraine after Taking out a Line of Russian Tanks," ABC News, August 25, 2022, https://abcnews.go.com/International/drone-boy-hero-ukraine-taking-line-russian-tanks/story?id=88740689.

artillery, who "decimated the column of Russian tanks within minutes."[101] *In addition to Drone Boy, the civilian-owned Starlink has provided Ukrainian forces with unprecedented capabilities to communicate and coordinate attacks in the ongoing conflict. Both Drone Boy and Starlink present unique distinguishability challenges concerning modern warfare, their ability to affect the battlefield, and the legitimacy of themselves becoming a target.*

In the proportionality case study, the technology was inherently dual-use. However, this case study offers a different viewpoint and questions when a person or technology is no longer a civilian entity and thereby loses its protected status. This transition makes it difficult for adversaries to correctly and distinctly differentiate military from civilian targets and blurs the line in what constitutes directly participating in hostilities.[102] The demarcation line for directly participating in hostilities has become precipitously thin and is only eroding with technological advancements. In an era where many scholars sought to remove humans from the battlefield, we are doing anything but.

For decades, militaries have grappled with civilian influence on the battlefield. However, their actions were removed from the front lines, and "traditionally, only a small minority of civilians became involved in the conduct of military operations."[103] Warfare today sees both a deliberate and natural "intermingling of civilians with armed actors."[104] Compounding this problem "is the blurring, flattening, and expanding of the battlefield brought about by new technology."[105] Legal advisor to the ICRC, Kubo Mačák, acknowledges that "the growing involvement of civilians in activities on the digital battlefield puts individuals at risk of harm and contributes to the erosion of the principle of distinction."[106] This fundamental shift affects not only how wars are conducted, but also

[101] Moscufo.

[102] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 260.

[103] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Geneva: International Committee of the Red Cross, 2009), 11.

[104] Melzer, 11.

[105] Matthew King, "High-Tech Civilians, Participation in Hostilities, and Criminal Liability," in *The Impact of Emerging Technologies on the Law of Armed Conflict*, ed. Ronald Alcala and Eric Jensen (New York: Oxford University Press, 2019), 176.

[106] Mačák and Vignati, "Civilianization of Digital Operations."

how definitions and distinctions between combatants and civilians are critical to just and ethical conduct in war.

Article 51 of Additional Protocol 1 states that civilians are non-combatants and are protected entities "unless and for such time as they take a direct part in hostilities."[107] This protection of civilians is not only codified in AP-1; it is also, according to Mačák, customary international law.[108] However, like all legal documents, there is room for interpretation on what constitutes combatant versus civilian and directly participating in hostilities. The ICRC provided interpretive guidance on the notion of direct participation of hostilities, which outlines the organization's view, under the guise of IHL, on the aforementioned topics. In addition to the interpretive guidance, the U.S. Law of War manual proposes a concurrent yet somewhat divergent view. Both frameworks and lenses will be applied to the case study regarding Drone Boy.

a. ICRC's Interpretive Guidance

Under IHL, civilians are rightly given vast amounts of deference to shield them from the horrors of war. IHL defines civilians as "all persons who are neither members of the armed forces of a party to the conflict nor participants in a *levee en masse*."[109] Furthermore, Article 50 of AP-1 provides the aforementioned deference where in "case of doubt whether a person is a civilian, that person shall be considered to be a civilian."[110] While *Drone Boy* is unquestionably a civilian, the question comes down to when, and if,

[107] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 265.

[108] Mačák and Vignati, "Civilianization of Digital Operations."

[109] Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 20. Melzer, in concurrence with AP-1 states: "as far as the levée en masse is concerned, all relevant instruments are based on the same definition, which refers to the inhabitants of a non-occupied territory who, on the approach of the enemy, spontaneously take up arms to resist the invading forces without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war. Participants in a levée en masse are the only armed actors who are excluded from the civilian population although, by definition, they operate spontaneously and lack sufficient organization and command to qualify as members of the armed forces. all other persons who directly participate in hostilities on a merely spontaneous, sporadic or unorganized basis must be regarded as civilians."

[110] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 265.

he loses his protection against direct attacks by injecting himself into the conflict. It is important to note that even if he loses his protection, *Drone Boy* does not become a combatant, targetable under those definitions of war, but retains a civilian who has lost "protection against direct attack for the duration of each specific act amounting to direct participation in hostilities."[111]

The interpretive guidance acknowledges the limited treaty definitions for direct participation in hostilities.[112] The guidance first clarifies the "for such a time" and "direct" portion of AP-1, Article 51, wherein civilians lose their protection "for such a time as they take a direct part in hostilities."[113] The guidance discusses that civilians will only use their protection for the duration in which they are actively engaging in "specific hostile acts."[114] This "temporary, activity-based loss of protection" is different for civilians than combatants and yields a revolving door dilemma that will be addressed in a subsequent section.[115] The intent behind the initial section of this interpretive guidance is that it underscores that direct participation in hostilities "does not refer to a person's status, function or affiliation, but to his or her engagement in specific hostile acts."[116] The interpretive guidance then provides a three-tier test to define whether a civilian's specific act constitutes a direct participation in hostilities.

The interpretive guidance, written on behalf of the ICRC, notes that in order for civilian acts to rise to the level of direct participation in hostilities, they must meet these requirements: "(1) a threshold regarding the harm likely to result from the act, (2) a relationship of direct causation between the act and the expected harm, and (3) a belligerent

[111] Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 70.

[112] Melzer, 41.

[113] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 265.

[114] Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 44.

[115] Melzer, 45.

[116] Melzer, 44.

nexus between the act and the hostilities conducted between the parties to an armed conflict."[117]

(1) Requirement: Threshold of Harm:

> In order to reach the required threshold of harm, a specific act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack.[118]

The threshold of harm argument expands the typically held view of harm being identified as death, injury, or destruction to persons and property to also include specific acts that "affect the military operations."[119] This expanded definition of the threshold of harm permits that "essentially any consequence adversely affecting the military" satisfies this first requirement.[120] The ICRC acknowledges that "transmitting tactical targeting intelligence for a specific attack" is an example of causing harm.[121] In the case of *Drone Boy*, the voluntary, operational intelligence he provided to Ukrainian forces proved critical and resulted in the death and destruction of an enemy tank column, therefore satisfying the requirement of the threshold of harm.

(2) Requirement: Direct Causal Link:

> In order for the requirement of direct causation to be satisfied, there must be a direct causal link between a specific act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part.[122]

---

[117] Melzer, 46.

[118] Melzer, 47.

[119] Melzer, 51.

[120] Melzer, 47.

[121] "Direct Participation in Hostilities: Questions & Answers," International Committee of the Red Cross, February 6, 2009, https://www.icrc.org/en/doc/resources/documents/faq/direct-participation-ihl-faq-020609.htm.

[122] Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 51.

While the threshold of harm nexus may be viewed as loose or over-encompassing, the second requirement seeks to reign that in by defining direct and indirect causal links to specific acts. The guidance differentiates between efforts that are part of the general war effort (resulting in an indirect causal link) and those that directly contribute and provide a "sufficiently close causal relation between the act and the resulting harm."[123] According to the ICRC guidance, the sufficiently close causal relation is that "the harm in question must be brought about in one causal step."[124] Under this guidance, the ICRC acknowledges that the "identification and marking of targets" and the "transmission of tactical intelligence to attacking forces" directly correlate to combat operations.[125] The U.S. Air Force defines its Special Reconnaissance personnel as those who "collect and exploit key information, develop targets, and tilt the battlespace in our favor."[126] *Drone Boy* was acting in a manner akin to Special Reconnaissance and provided integral tactical intelligence to Ukrainian forces. The ICRC acknowledges that tactical intelligence does not directly cause harm in isolation, but the "requirement of direct causation would still be fulfilled where the act constitutes an integral part of a concrete and coordinated tactical operation that directly causes such harm."[127] The assistance *Drone Boy* gave to Ukrainian forces directly contributed to the death and destruction of Russian forces.

(3) Requirement: Belligerent Nexus:

> In order to meet the requirement of belligerent nexus, an act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another.[128]

Belligerent nexus exists when the specific act was designed to directly cause harm and is independent of the state of mind, but rather dependent on the "objective purpose of

[123] Melzer, 52.

[124] Melzer, 52.

[125] Melzer, 55.

[126] "Special Reconnaissance," U.S. Air Force, accessed October 16, 2023, https://www.airforce.com/careers/combat-and-warfare/special-warfare/special-reconnaissance.

[127] Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 55.

[128] Melzer, 58.

the act."[129] *Drone Boy* acknowledges that he had "mixed feelings" about voluntarily providing the critical targeting intelligence as the attack as Russians were killed (intent). However, his objective "was to find the exact coordinates and pass them on to the soldiers," where they were then able to destroy the Russian tank column.[130] Furthermore, the Ukrainian commander who recruited *Drone Boy* acknowledged that he was "the only one who was experienced with drones in that region" and that he voluntarily helped the Ukrainian army to prevent Russian progress, clearly and unequivocally supporting one party to the detriment of another.[131]

After assessing *Drone Boy's* actions through all three requirements for direct participation in hostilities, an argument can be made that he directly participated in hostilities when he was conducting the specific act of flying the drone overhead and providing intelligence to the Ukrainian army. When he was actively providing special reconnaissance to the military, he lost his protected status as a civilian and was, therefore, subject to direct attack. However, questions arise as to when he is no longer actively conducting the action of providing intelligence to Ukrainian forces. May he assume the child by day and fighter by night moniker and be protected when he is not flying his drone? The ICRC unquestionably says, yes.

(4) Revolving Door

The Interpretive Guidance acknowledges the "revolving door" of civilian protection wherein suspension of a civilian's rights against targeting "lasts exactly as long as the corresponding civilian engagement in direct participation of hostilities."[132] This extreme deference to civilian protection, wherein they lose and regain protection

[129] Melzer, 59.

[130] Ministry of Foreign Affairs of Ukraine, "15-Year-Old Andrii Helped Destroy a Column of Russian Equipment Thanks to His Drone Skills," June 2022, https://war.ukraine.ua/heroes/15-year-old-andrii-helped-destroy-a-column-of-russian-equipment-thanks-to-his-drone-skills/.

[131] Catherine Stoddard, "15-Year-Old Ukrainian Boy Dubbed a Hero after Using Drone to Help Defeat Russian Forces," *Fox 32 Chicago*, June 8, 2022, https://www.fox32chicago.com/news/15-year-old-ukrainian-boy-dubbed-a-hero-after-using-drone-to-help-defeat-russian-forces-report.

[132] Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 70.

repeatedly, is an "integral part, not a malfunction, of IHL," the ICRC argues.[133] The only way for a civilian to be lawfully targeted when not actively engaged would be for that civilian to change their class altogether and become either a lawful combatant or a participant in a levee en masse situation. By recognizing the complications of a civilian, non-combatant, becoming a lawful target off-and-on, the ICRC dismisses such complexities, holding the view that the revolving door "remains necessary to protect the civilian population from erroneous or arbitrary attack," consequently, the U.S. Law of War Manual does not hold its military to this belief.[134]

b. DOD Law of War Manual

When assessing whether a civilian is taking a direct part in hostilities, the U.S. Department of Defense acknowledges the presence of AP1's definition, yet asserts that the U.S. has not ratified AP1 and, therefore, "has not adopted the direct participation in hostilities rule."[135] Furthermore, the manual asserts, to the disagreement of many in the international community, that Article 51 of AP1 "does not reflect customary international law" and is therefore unbounded by the rules and regulations contained therein.[136] Nonetheless, the manual provides a framework for military leaders to assess whether a civilian is taking a direct part in hostilities.

Ironically, the framework provided in the manual follows closely to the overall framework proposed in the ICRC Interim Guidance. The U.S. framework provides five lenses: 1) "the degree to which the act causes harm to opposing party's persons or objects" (similar to the Interim Guidance requirement of threshold of harm), 2) "the degree to which the act is connected to the hostilities" (similar to the Interim Guidance requirement of causal link), 3) "the specific purpose underlying the act" (belligerent nexus), 4) "the military significance of the activity to the party's war effort" (belligerent nexus), and 5) "the degree to which the activity is viewed inherently or traditionally as a military one"

[133] Melzer, 70.

[134] Melzer, 71.

[135] Department of Defense, *Law of War Manual*, 234.

[136] Department of Defense, 235.

(belligerent nexus).[137] Due to their similarities to the Interim Guidance, the U.S. mostly follows the intent of AP1. However, the manual also gives examples of civilians taking a direct part in hostilities and when they have lost their protected status.

One example the manual provides is individuals "providing or relaying information of immediate use in combat operations."[138] The manual goes on to specify that if airstrikes or other attacks are a direct result of the information relayed, then that individual would be considered directly participating in hostilities and, therefore, deprive any participating civilians of protection.[139] The direct, voluntary, and acknowledged effort of Drone Boy would, according to the DOD Law of War Manual, be seen as directly participating in hostilities. While the Law of War Manual and Interim Guidance agree on this, they differ regarding the revolving door analogy.

The DOD Law of War Manual directly and unambiguously states that there is no revolving door of protection unless they permanently cease their actions.[140] According to the manual, there is no "farmer by day, fighter by night" protection for such individuals.[141] Instead, the U.S. maintains that if civilians habitually engage in conduct commensurate with a military act, then they "do not regain protection from being made the object of attack in the time period between instances of taking a direct part in hostilities."[142] The manual simply asks that commanders make a "good faith assessment" to predict future action on behalf of the civilian.[143] This judgment is precisely what the ICRC seeks to avoid as they assert that there are no clear and reliable predictions as to the future conduct of a civilian.[144] The interpretive guidance gives a wide latitude of deference to the civilian

[137] Department of Defense, 238.

[138] Department of Defense, 240.

[139] Department of Defense, 239.

[140] Department of Defense, 242.

[141] Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 72.

[142] Department of Defense, *Law of War Manual*, 243.

[143] Department of Defense, 243.

[144] Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 71.

population, wherein the U.S. seeks to extrapolate human behavior as future indicators. In any case, both agree that when actively conducting a specific act, such as providing tactical intelligence to facilitate a strike on a Russian tank column as done by Drone Boy, then civilians are directly participating in hostilities and have lost protection from a deliberate and distinct attack.

The above example focused on the distinction between a civilian who is directly participating in hostilities. Questions arise on not whether a civilian is directly participating in hostilities and therefore at a loss for protection, but rather certain objects or capabilities of a civilian nature that perform military-style tasks. One such example is the Ukrainian military leveraging Starlink satellites to not only enhance its command, control, communications, and intelligence (C3I) infrastructure but also directly enable airstrikes against the enemy. In using the above framework from the ICRC Interpretive guidance, while Elon Musk might not lose his protected status as a civilian (due to a lack of direct causal link), the satellites he provides would likely lose their protection as civilian assets and are, therefore legitimate military targets under international law.

Should the Starlink satellite network be targeted, either through an expanding ASAT capability, lasers, or even cyber attacks, a traditional jus in bello analysis of proportionality and distinction must be undertaken where the benefits of removing a dual-use capability from the battlefield are proportionate to the military objectives achieved. What was once seen as being used only for "peaceful purposes," as outlined in the Outer Space Treaty of 1967, space has not only become increasingly militarized but also fused with civilian and dual-use functions.[145] What started off, and continues to be, a commercial satellite communications network, Starlink has become an integral part of Ukraine's C3I enterprise, wherein Ukrainian digital minister Mykhailo Federov acknowledged, "Starlink is indeed the blood of our entire communication infrastructure now."[146] In response to the advantage Starlink gives Ukraine, a senior Russian foreign minister warned that "quasi-

[145] Treaty Banning Nuclear Weapon Tests in the Atmosphere, In Outer Space and Under Water, U.S.-U.K.-U.S.S.R., Aug. 5, 1963, 14 U.S.T. 1313. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html.

[146] Adam Satariano et al., "Elon Musk's Unmatched Power in the Stars," *The New York Times*, July 28, 2023, https://www.nytimes.com/interactive/2023/07/28/business/starlink.html.

civilian infrastructure may become a legitimate target for retaliation."[147] It is clear that the Russian interpretation of distinction is that these satellites are directly contributing to the war effort and, therefore, have lost their protected status as civilian objects. Elon Musk, CEO of Starlink, appears to be cognizant of this latent threat as there have been multiple instances where he would cut off the Starlink feed to certain regions of Ukraine when he feared that the network would be used to "cause significant military casualties."[148] This ability for one man, or any private company, to affect the battlefield is a stark departure from norms and is changing the security dynamic of dual-use technology. The world may quickly find itself in a new era, where civilian entities become the lords of war and international customers and militaries are beholden to the whims of civilian entities that may or may not align with strategic interests.

E. A NEW JWT APPROACH.

The blurred lines between state actors, non-state actors, and civilian influence on the battlefield challenges traditionally held views on just war theory. The breakdown in what constitutes *jus ad bellum* and *jus in bello* justification in war is a result of increased individual and non-state actors in the arena. Traditional JWT contends that collective organizations or groups go to war and are subject to both *jus ad bellum* and *jus in bello* principles of war. On the other hand, traditional JWT also contends that individual combatants are responsible only for adhering to *jus in bello* principles, not *jus ad bellum* ones. This differentiation is traditionally held as individual combatants are not those who make the *jus ad bellum* decisions to go to war in the first place. Instead, they are merely responsible for adhering to the laws of war in conducting any combat they engage in "within their own sphere of activity."[149]

[147] Kari Bingen, Kaitlyn Johnson, and Makena Young, "Space Threat Assessment 2023" (Washington, DC: Center for Strategic and International Studies, April 2023), 17, https://www.csis.org/analysis/space-threat-assessment-2023.

[148] Satariano et al., "Elon Musk's Unmatched Power in the Stars."

[149] Walzer, *Just and Unjust Wars*, 38.

Furthermore, the traditionalist view holds that in wars, moral equality exists amongst combatants on both sides of a conflict.[150]This equality exists even if the members of one side of a conflict are engaged in an unjust war by *jus ad bellum* principles; combatants on both sides are on equal moral ground when they engage one another in combat and are equally liable to be harmed by the other. However, a recently resurgent revisionist school of just war theory argues that this separation of moral responsibility for the individual from the cause for which they fight is archaic and incoherent. Rather, individuals need to be held accountable for their actions, not only for how they behave in war, but for their decision to fight for the cause of war as well. This logic results in a rejection of the moral equality of combatants held by the traditional camp and has significant implications on how we should morally understand both distinction and proportionality in war.

While a complete exposition of the implications of revisionist just war theory is beyond the scope of this thesis, a couple of quick comments are in order. On a revisionist approach, the cases analyzed above would be pushed for different conclusions. For the Aggresistan example, revisionists would assert that they are not fighting for a just cause and that there is no equal moral footing for the combatants engaged in conflict. Moreover, they would seek to hold not just the nation accountable, but the civilians who encouraged conflict as "they can be instigators of unjust wars, or aiders and abettors who share responsibility for unjust acts of war perpetrated by unjust combatants."[151] Revisionists discard the collective security of the state and instead acknowledge that "civilians may have a high degree of responsibility for an unjust war," thereby breaking down the previously held barrier of *jus ad bellum* principles only applying to a state actor.[152]

For those fighting on behalf of the *just ad bellum* just cause in the Ukraine/Russia war, the Ukrainians, who are defending against unjust aggression, would not be in morally symmetrical standing to the Russian combatants who are fighting for an unjust cause. This,

[150] Walzer, 34.

[151] Jeff McMahan, *Killing in War* (Oxford: Oxford University Press, 2011), 208.

[152] McMahan, 214.

in turn, would imply that Drone Boy, while fighting on behalf of the Ukrainian cause, is doing so justly. And so long as his actions therein adhere to the strictures of *jus in bello*, he would not be liable to the unjust harm of the Russian combatants. Meanwhile, the Russians, fighting for an unjust cause, would be liable to attack to repel their unjust war aims. Such a view shifts the designation of liable target away from simply who is fighting or contributing, but to the justification for that contribution in the first place.

Lastly, a revisionism argument holds that "civilian immunity is contingent rather than absolute."[153] This immunity is an essential distinction as orthodox just war theory contends that liability falls with membership, not with an action. However, membership (be it a state actor or even the military) is no longer critical to employ significant effects against an adversary. This power is seen with the capability Elon Musk and Starlink have independently provided to the Ukrainians and how Elon himself has wondered, "How am I in this war?"[154]

Legally, of course, the ICRC and IHL generally wish to remain neutral on matters of *jus ad bellum* responsibility. And they do so precisely because they wish to adjudicate to both sides in a conflict the rules of *jus in bello* warfare and, therefore, apply an equal "*legal* equality of combatants."[155] Morally, however, the revisionist case, in one sense, complicates the matter of dual-use distinction, and, in another sense, simplifies it by tying it to the just (or unjust) cause in the first place.

F. CONCLUSION

The convergence of the principles contained within modern JWT and dual-use capabilities rapidly becomes an issue in modern ethics, as dual-use capabilities blur the line between civilian and military objectives. This convergence calls into question the definition of a legitimate military objective, as technological advancements have dramatically affected the ability to wage and influence war. Traditional JWT offers insight

[153] McMahan, 231.

[154] Walter Isaacson, *Elon Musk* (New York: Simon & Schuster, 2023), 434.

[155] McMahan, *Killing in War*, 105.

into the morality of why wars are initiated and how they are conducted, however, the traditional view is applied through the lens of state-on-state actors. New capabilities have thus entangled civilians and their equipment into conflicts not seen before. Some approaches of Just War Theory revisionism seek to break down the barrier of civilian immunity and, in turn, look to the action being conducted rather than who, or what organization, is conducting it. However, the moral and ethical dilemma facing dual-use technology is but one of a greater argument regarding how these new advancements affect the security and stability of the United States.

III. DUAL-USE CAPABILITIES AND U.S. NATIONAL SECURITY

Just as distinction and discrimination are critical to the morality of attacking a threat or a target, a lack of distinguishability negatively affects U.S. security as it increases the possibility of conflict and competition. In addition to a lack of distinguishability, both new technology and civilian capabilities have become highly integrated into the enterprise, and the boundary of war is largely indistinct. Dual-use technology and the civilians that wield it are both victims and participants.

This lack of distinguishability and increased integration results in a security dilemma for the U.S. that manifests itself in the deliberate co-mingling of assets, resulting in decreased detection and attribution capabilities that may negatively affect U.S. optics at home and abroad. This convergence, coupled with an increased usage of commercial technology, is "leading to a revolution in military affairs."[156] This rapid change in the status quo enables U.S. adversaries like China to leverage the dual-use obfuscation to their advantage to, according to the National Security Strategy, "reshape the international order."[157] The People's Republic of China seeks to expand its "technological capacity" and thus rapidly modernize its military.[158] They seek to accomplish that feat by leveraging fusion between its civilian and military enterprises. The fusion has now resulted in not only an ethical issue, as mentioned previously, but also a security dilemma where U.S. policymakers have not yet understood the ramifications of complacency.

A. DISTINGUISHABILITY VERSUS INTEGRATION

In their recently published article on *Dual Use Deception*, Jane Vaynman and Tristan Volpe offer a framework for analyzing the dual-use nature of technology and its potential impact on international cooperation.[159] The framework characterizes technology

[156] T.X. Hammes, "The Tactical Defense Becomes Dominant Again," *Joint Forces Quarterly* 103, no. 4 (2021): 10, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2807244/the-tactical-defense-becomes-dominant-again/.

[157] Biden, *National Security Strategy of the United States of America*, 23.

[158] Biden, 23.

[159] Vaynman and Volpe, "Dual Use Deception," 603–4.

amongst two dimensions: distinguishability and integration.[160] The degrees of distinguishability and integration play a pivotal role in determining the employment of a capability within civilian, military, or joint operations.

Distinguishability, as it relates to dual-use technology, refers to the "relative ease of differentiating between a technology's military and civilian applications."[161] For years, military aircraft have sported a roundel to differentiate themselves from their civilian counterparts (as if the camouflage paint and missiles under the wings did not already do so). These distinct physical characteristics are easy to identify and distinguish military from civilian assets. However, other capabilities do not present overt physical characteristics. For example, SpaceX's Falcon9 rocket launches secret spy satellites in the same manner as it can deploy purely academic and scientific ones.

In addition to the lack of physical characteristics, Vaynman and Volpe assert that if a development pathway for a civilian capability aligns with the military one, it is difficult to distinguish the military or civilian asset.[162] If these pathways overlap throughout production (as is the case for nuclear development for peaceful energy generation or a weapon), it adds to the indistinguishability paradox. Conversely, disparate developmental pathways, exemplified by the SR-71 Blackbird originating from Lockheed's Skunk Works, utilized distinct titanium-based tools and avant-garde manufacturing methodologies, which stood in stark contrast to the techniques and tools utilized for Lockheed's commercial L-1011 TriStar aircraft.[163]

Next to affect the distinguishability of a capability is the deployment and doctrinal methods of employment.[164] Underground silos and solid-state rocket propellants made it abundantly clear during the Cold War that those facilities were different than their NASA

[160] Vaynman and Volpe, 600.

[161] Vaynman and Volpe, 600.

[162] Vaynman and Volpe, 605.

[163] Peter Merlin, "Design and Development of the Blackbird: Challenges and Lessons Learned," in *47th AIAA Aerospace Sciences Meeting* (47th AIAA Aerospace Sciences Meeting, Orlando, FL: American Institute of Aeronautics and Astronautics, 2009), 16, https://doi.org/10.2514/6.2009-1522.

[164] Vaynman and Volpe, "Dual Use Deception," 605.

counterparts at Cape Canaveral. However, as mentioned earlier, SpaceX's inherent dual-use nature leverages both U.S. military installations (e.g., Vandenberg Space Force Base) and non-DOD locations (e.g., the NASA-owned Kennedy Space Center) to launch both civilian satellites (e.g., Starlink) as well as classified National Reconnaissance Office spy satellites.[165] When doctrinally employed in the same manner, civilian versus military distinguishability is extremely low.

Lastly, the conversion speed, or latency, identifies the cost of transitioning "civilian capabilities into military assets."[166] While the cost may include money and time, the ability of the government to transition from civilian to military and back again causes a *What if?* dilemma for the adversary. A quicker transition period, or lower latency, results in an asset that will cause security and operational issues. The Chinese People's Liberation Army is leveraging small amounts of latency in its commercial car ferries by using them to employ and recover their military's amphibious vehicles.[167]

A lack of distinguishability amongst the four aforementioned characteristics increases the severity of competition and calls into question the ethics of employment and deception. Current doctrinal practices amongst numerous nations are to take longstanding distinguishable assets and manipulate them to their advantage. The CCP is doing this with their aforementioned commercial ferry vessels.[168] The Russians have developed the Klub-K anti-ship missile system, a standard commercial shipping container designed to look innocuous yet engage land and sea-based targets.[169] The weapon's indistinguishable nature permits them to hide in plain sight and proves challenging to differentiate them from a commercial container. Not immune from leveraging the changing nature of

[165] Stephen Clark, "NRO Reveals Plans for Previously-Undisclosed SpaceX Launch This Month," Spaceflight Now, October 5, 2020, https://spaceflightnow.com/2020/10/05/nro-reveals-plans-for-previously-undisclosed-launch-with-spacex-this-month/.

[166] Vaynman and Volpe, "Dual Use Deception," 605.

[167] Courtney Mabeus, "Chinese Navy Using Commercial Car Ferries to Launch Amphibious Landing Craft," USNI News, July 26, 2021, https://news.usni.org/2021/07/26/chinese-navy-using-commercial-car-ferries-to-launch-amphibious-landing-craft.

[168] Mabeus.

[169] Global Security, "3M-54 Klub," Global Security, accessed November 1, 2023, https://www.globalsecurity.org/military/world/russia/club.htm.

indistinguishability, U.S. prime contractor Northrup Grumman is also pursuing containerized missile systems.[170] In addition, the United States Air Force has sought to have the ability to rapidly convert benign airlift platforms in order to employ palletized Joint Air-to-Surface Standoff Missiles with their Rapid Dragon Program, essentially making every cargo plane a bomber.[171] The indistinguishable nature of emerging capabilities is a far cry from the roundel-carrying military assets of yesteryear, thereby presenting security challenges around the unknown, where the stakes of wrongful classification are high.

In addition to distinguishability, another factor that affects the dual-use dilemma is how well integrated a capability is within the civilian and military enterprises. Vaynman and Volpe assert that "technology's pervasiveness reflects its range and depth of use in each realm."[172] Technology not integrated amongst the civilian and military enterprises is often niche or isolated capabilities suited to only one primary market. However, highly integrated technologies are pervasive in both spheres and represent current technological trends. Historically, critical technological improvements have first been generated in the military sphere and adapted to civilian use. However, a shift is afoot where the military seeks to lower its research and development demand, have the commercial technology bear risk, and drive down overall costs. A case in point is the convergence of cyber and space domains, as they are deeply intertwined with both military and civilian cultures. Not only was this entanglement a natural transition of dual-use technology, but some states are seeking to deliberately increase integration, resulting in critical dilemmas for national security.

[170] Tyler Rogoway, "Northrop Grumman Shows Off Shipping Container-Launched Anti-Radiation Missile Concept," The Drive, October 8, 2018, https://www.thedrive.com/the-war-zone/24111/northrop-grumman-shows-off-shipping-container-launched-anti-radiation-missile-concept.

[171] "Rapid Dragon," Air Force Research Laboratory, accessed November 1, 2023, https://afresearchlab.com/technology/rapid-dragon.

[172] Vaynman and Volpe, "Dual Use Deception," 607.

B. CHANGING NATURE OF DUAL-USE TECH

Following a categorization of technological capability (level of distinguishability and integration), Vaynman and Volpe formed a 2x2 grid wherein capabilities that are both highly indistinguishable and highly integrated form a "dead zone" that limits the potential for cooperation and maximizes interstate competition.[173] In this dead zone, one can find many advanced technological improvements affecting the battlefield today, including space, cyber, and Artificial Intelligence. A genuine concern is that state actors, non-state actors, and even individuals can leverage this dead zone, which would shape worldwide competition. Dead zone technologies are at the heart of competition and are highly integrated within both military and civilian institutions, thereby decreasing any prospects of cooperation or management. While this might be beneficial as it could help anticipate what an adversary might be investing research and development money in, the concern is that organizations such as the PRC are leveraging technology that used to be highly distinguishable (e.g., merchant marine vessels), and using this longstanding attribute as cover to pursue other nefarious capabilities. This shift represents a changing tide of attributes, obscuring the understood left and right bounds of technology and capability.

This increase in indistinguishability, coupled with high levels of integration, presents a dilemma. While it is imperative for countries to prevent adversaries from exploiting dual-use technologies, harnessing its potential for their own beneficial purposes remains equally essential. The last few decades have seen a big push in the Western defense community to develop tech in a purposefully integrated manner. This dedicated attempt, to encourage commercial actors to lead the way concerning technological innovation, permits the Department of Defense to lower its research and development costs and spin-off military capabilities from civilian applications. By leveraging and relying upon the dual-use nature of new capabilities, a government can sidestep the classic guns-vs-butter dilemma where it must spend money on either defense applications or domestic

[173] Vaynman and Volpe, 601. Areas that are of low integration, but high distinguishability represents the "permissive zone" wherein the best prospects for cooperation exist. Capabilities that have high levels of integration yet high levels of distinguishability ("disclosure constraint") or ones that have low levels of integration yet low distinguishability ("Detection constraint") represent modest prospects for cooperation.

improvements while sacrificing the unfunded.[174] While this has many advantages, the more that nations compete over highly integrated technology, the more difficult it will be to manage capabilities (e.g., arms racing, international agreements, and norms). This difficulty could fuel greater competition with adversary countries.

In addition to the guns-vs-butter situation, such integration also lowers the threshold of involvement for non-combatants. Consequently, non-state entities or individuals can exert influence without being under governmental oversight. A highly integrated tech sector with dual-use government and civilian applications may result in the potential for an adversary to obtain parallel access to the commercial tech (through standard capitalism business deals or espionage) and rapidly leverage the latency built into such a capability, quickly turning it into a military asset.[175] The U.S. needs to reevaluate adversary peddling in the commercial field. A recent Pentagon study found that "nearly all cases show that China, not the U.S., is the ultimate beneficiary of DOD and other U.S. government research investments."[176] This alarming transition illuminates the effect that dual-use technology is having and presents real security dilemmas for the United States.

C. SECURITY DILEMMA

The lack of distinguishability and integration enjoyed by many dual-use capabilities presents a security dilemma for the United States that manifests itself in a deliberate co-mingling of capabilities dilemma, a detection dilemma, an attribution dilemma, and an optics dilemma. These four issues all present unique security characteristics that will affect how the U.S. responds to adversarial action in the event of a conflict or sustained competition.

[174] Tom Becker, "Guns and Butter 2.0," BlackRock, March 8, 2023, https://www.blackrock.com/us/individual/insights/guns-and-butter.

[175] For more information on latency regarding nuclear weapons technology, reference Tristan Volpe's *Leveraging Latency: How the Weak Compel the Strong with Nuclear Technology.*

[176] Charles Wessner and Sujai Shivakumar, *Renew SBIR, Just Defend the Recipients against China* (Washington, DC: Center for Strategic & International Studies, 2022), https://www.csis.org/analysis/renew-sbir-just-defend-recipients-against-china.

Conventional international relations theory purports that when two nations are at odds with one another, countries will seek to attack only their opponents' conventional assets while leaving their nuclear assets untouched for fear of escalating into a nuclear war. Historically, distinguishability between conventional assets and nuclear capabilities was not an issue as the nuclear "technology often ends up sequestered away from other capabilities."[177] Recent trends have been to deliberately co-mingle conventional and nuclear assets to, potentially, protect both capabilities from an attack. However, doing so exacerbates "the risk of inadvertent escalation."[178] This entanglement would force the U.S. into the horns of a dilemma where, while its procedure might be to target conventional Command and Control nodes while leaving nuclear ones alone, the co-mingling of assets renders it difficult to target only conventional capabilities. As a result, adversary forces might perceive that the U.S. is targeting its nuclear infrastructure and, thereby, vastly escalating the conflict. The co-mingling of capabilities extends beyond the conventional versus nuclear realm and encompasses the civilian versus military domains. By being highly indistinguishable and integrated, dual-use capabilities present detection, attribution, and optics dilemmas for the United States.

The fusion of dual-use military and civilian technologies drives a detection dilemma, as decision-makers will not know until it is too late if an asset is genuinely civilian or has a latent military capability. During the Cold War, the USSR feared that the NASA Space Shuttle program was a front to deliver nuclear payloads to Moscow.[179] A report written in 1976 by the department head at the Institute of Applied Mathematics in Moscow asserted that the shuttle "could make a dive in its orbit as it passed over Moscow, and release a nuclear weapon" which would deliver such a weapon in mere seconds vice minutes for the expected delivery methods of a submarine-launched ballistic missile.[180]

[177] Vaynman and Volpe, "Dual Use Deception," 609.

[178] James Acton, "Summary," in *Entanglement: Chinese and Russian Perspectives on Non-Nuclear Weapons and Nuclear Risks*, ed. James Acton (Carnegie Endowment for International Peace, 2017), 1, https://carnegieendowment.org/2017/11/08/underappreciated-risks-of-entanglement-chinese-perspective-pub-73164.

[179] Vaynman and Volpe, "Dual Use Deception."

[180] Dwane Day, "Nuking Moscow with a Space Shuttle," The Space Review, December 23, 2019, https://www.thespacereview.com/article/3855/1.

While far from the truth, this fear escalated and heightened tensions between the two nations. Dual-use capabilities may similarly manifest themselves.

Similar to dual-use biological weapons, where it is hard to distinguish whether one is working towards peaceful ends of antibodies and defenses or weaponizing agents, modern-day technology presents similar fears that the world has grappled with for decades. Except in today's world, the grappling is literal. Advanced developments in space have led countries to find creative ways to service and repair space-based assets. Though this technology appears innocuous and employed solely for peaceful endeavors, its underlying potential for physical attacks remains concealed at the surface. In a 2023 statement to the House Armed Services Committee, U.S. Space Command Commander, General Dickinson, acknowledged that China has exhibited the capability to "grapple satellites with its robotic arm-equipped satellites" and reposition them into a "grave-yard orbit."[181] This skill demonstrates an understandably needed ability to remove out-of-date or decommissioned satellites from orbit. However, this same robotic arm could be used in times of escalation or conflict to diminish U.S. capabilities in space. This coercive factor has a deterrent element, as "deterrence succeeds by altering the cost-benefit calculus of a potential aggressor."[182] As a result, the United States has amplified its Space Domain Awareness program to detect any "unusual and threatening behaviors" as "no orbital regime is out of reach of counterspace weapons."[183] However, distinguishing whether a new capability has a dual-use or benign functionality will be difficult as, in the case of China, "the line between commercial and governmental endeavors is often blurred by Beijing's military-civilian fusion policy" that encourages such enterprises to "achieve both economic and military dominance."[184] Due to the lack of distinction, the U.S. will no longer be able to respond to a *deployment*, but may now have to react to an adversarial

[181] *Examining Irregularity in the Strategic Basing Process for U.S. Space Command: Testimony before the House Armed Services Committee,* 118th Cong. 1 (2023) (statement of General James H. Dickinson, Commander, United States Space Command).

[182] Bingen, Johnson, and Young, "Space Threat Assessment 2023," 37.

[183] Bingen, Johnson, and Young, 37.

[184] Bingen, Johnson, and Young, 9.

employment of a capability. However, this also faces problems of attribution (who is doing it?) and timing (is it too late?).

The issue of attribution remains persistent in the realm of dual-use technology and capabilities, making it challenging to discern whether an attack originated from an adversarial nation, a non-state entity, or a singular aggrieved individual. This complication arises due to digital spaces' anonymity, allowing entities to operate without clearly revealing their affiliations. As a result, determining responsibility for cyber incidents becomes a delicate endeavor. The *Tallinn Manual on the Law in Relation to Cyber Operations* notes that mere origination within nor "state ownership is not alone sufficient to characterise [sic] a corporation as an organ of the state."[185] The manual postulates that this difficulty is primarily due to the private versus governmental distinction of whether such an act is under the "direction or control" of the state.[186] Whether a nation is actively or passively involved is an ever-present dilemma that permits governments to maintain plausible deniability. The ability of a nation-state to distance itself from any nefarious capability renders it very difficult for response options on behalf of the aggrieved country. Even if the victim has intelligence that supports the claim that a state actor was behind such an activity, it presents an information and security flow problem that could affect international perceptions and optics.

The deliberate entanglement of civilian and military forces and capabilities presents an optics dilemma, where reacting too aggressively might harm perceived civilian forces and draw international condemnation. However, reacting too leniently could compromise national security. This dilemma gives the adversary a distinct advantage. The aggrieved state forcibly walks on a tightrope where it must safeguard its national interests and deter future attacks, yet simultaneously counter a perception that they are an unruly aggressor attacking innocent civilian platforms. Even if the aggrieved state is *positive* that an asset is *not* dual-use but rather purely military, public perception may be swayed by statements made on behalf of the aggressor. For example, during the Chinese Spy balloon intrusion of

[185] Schmitt and Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 88.

[186] Schmitt and Vihul, 94.

the United States in 2023, the Chinese Ministry of Foreign Affairs issued a statement asserting that "the airship is for civilian use and entered the U.S. due to force majeure, which was completely accidental."[187] However, even though the Chinese balloon *was* very distinguishable as a military spy balloon, the counter-narrative was voiced, and states sympathetic to China condemned the U.S. for shooting down a "civilian aircraft."[188] Countering a narrative, no matter how boisterous, implausible, or flat-out wrong it may be, proves difficult in a time when allegiances and beliefs are closely held and often predetermined.

However, this is not just a game of cat and mouse between adversarial nations below the threshold of conflict. Instead, it has real implications for international norms and treaties. As Vaynman and Volpe allude to, the indistinguishable nature of many dual-use objects, coupled with their integration into all facets of military and civilian infrastructure, can result in an arms race where cooperation is counterproductive as there are no agreements or means to monitor the true intent behind a capability.[189] Leveraging this dead zone, in turn, creates complex dilemmas that increase organizational costs to counter the ever-present threat.

D. INDIVIDUAL SUPPORT DILEMMA

Not only do emerging dual-use capabilities present complications for a nation's national security, but they also present issues in the realm of individual support and culpability. The individual use of dual-use capabilities and influence can manifest in various ways. Three such ways are an unawareness of the clear and present danger individuals may inadvertently be subjecting themselves to, garnering power and influence

[187] Ministry of Foreign Affairs of the People's Republic of China."Statement on the US Claim of Shooting Down the Chinese Unmanned Airship."

[188] Dale Quinn, "Venezuela Condemns US for Shooting Down Chinese Balloon," *Bloomberg*, February 5, 2023, https://www.bloomberg.com/news/articles/2023-02-05/venezuela-condemns-us-for-shooting-down-chinese-balloon.

[189] Vaynman and Volpe, "Dual Use Deception," 627.

that amounts to a new *Lord of War*, or injecting themselves into a conflict for which the government cannot control or oversee their actions.[190]

While Drone Boy's actions were heroic and were in line with supporting his nation against an aggrieved attack, he was likely unaware that many states and organizations would interpret the law as stating that although he is a civilian, he has lost his protected status and is therefore liable for the attack. Although he acknowledged his mother was scared, alluding to the fact that there might be some recognition regarding the dangerous nature in which he was assisting the military, Drone Boy needed to be explicitly aware of the repercussions of direct civilian support.[191] The direct enlistment of help from the Ukrainian forces represents a treacherous path for individualized, non-combatant, support to the war effort and represents a stark departure from previous conflicts. The NDS acknowledges this behavior and notes the shifting battlespace, where "unclear norms of behavior" have changed kinetic conflict.[192] To protect and safeguard its citizens, governments need to be prescriptive and transparent about the risks associated with civilian recruitment for assistance in armed conflict.

Drone Boy's assistance to his country in a time of war was admirable and heroic, however, other individual injects may not be as righteous or unambiguous. Russia's invasion of Ukraine is the largest, unprovoked, unwarranted, and illegal act of state-on-state aggression since WWII. It has highlighted the potential capabilities individuals (not governments) can wield in international conflict, turning themselves into Lords of War. In his recent biography, Elon Musk asked, "How am I in this war? Starlink was not meant to be involved in wars. It was so people can…do good peaceful things, not drone strikes."[193] Nonetheless, Starlink became an integral part of Ukrainian Command and Control, and one

[190] The Lord of War moniker is in reference to the 2005 film. *Lord of War*, directed by Andrew Niccol (2005; Santa Monica, CA: Lions Gate Films, 2005), http://www.video.amazon.com.

[191] Michela Moscufo, "'Drone Boy' Becomes Hero in Ukraine after Taking out a Line of Russian Tanks," *ABC News*, August 2022, https://abcnews.go.com/International/drone-boy-hero-ukraine-taking-line-russian-tanks/story?id=88740689.

[192] Department of Defense, *National Defense Strategy of The United States of America*, 6.

[193] Walter Isaacson, *Elon Musk* (New York: Simon & Schuster, 2023), 434.

platoon commander noted that "without Starlink, we would have been losing the war."[194] While this instance was a noble pursuit, albeit a splendid real-world test for his new system, little precedent exists for an individual "becoming the arbiter of war between nations in such a granular way."[195]

Historically, when governments leverage dual-use technology on the battlefield, they do so through contractual commitments on the bounds of usage. By leveraging this deliberate bureaucracy, "a layer of protection exists between private companies and foreign governments."[196] However, the services provided by Starlink broke through these typical bureaucratic bounds to get the capability fielded faster. This technique resulted in immense power and influence in the hands of one man, Elon Musk. During one specific raid, where Ukraine was seeking to offensively strike a Russian target and use Starlink as its communication node, Musk "personally took charge of the situation" and "secretly told his engineers to turn off coverage," thus rendering the attack unsuccessful.[197] While Musk asserts this was due to an attempt to mitigate escalation between the two hostile nations, it exemplified that, when done incorrectly, civilian support to armed conflict results in unforeseen consequences. In this example, the significance of personal control of critical strategic assets directly affected the battlefield. By injecting himself into a war that neither the U.S. nor the Ukrainian government could control, Ukraine was, in essence, "living off his good graces."[198]

This lack of control presents a daunting reality where civilian influence on the battlefield eclipses that of state governments. When asked if he has more influence than the U.S. government, Elon replied, "in some ways."[199] The influence has resulted in a situation where, unlike in traditional defense contractor relationships, pure commercial

[194] Isaacson, 429.

[195] Ronan Farrow, "Elon Musk's Shadow Rule," *The New Yorker*, August 21, 2023, https://www.newyorker.com/magazine/2023/08/28/elon-musks-shadow-rule.

[196] Isaacson, *Elon Musk*, 2023, 432.

[197] Isaacson, 430.

[198] Farrow, "Elon Musk's Shadow Rule."

[199] Farrow.

influence may not "align with U.S. interests."[200] This is a slippery slope because the government is trying to balance the critical technology private organizations like SpaceX provide the U.S. government with their ability to influence the world order. The push to leverage commercial actors' technological assets for dual-use functions provides critical capabilities and redundancies for the defense department. For instance, the U.S. Space Force is finalizing a plan for "harnessing commercial satellite capabilities in times of crisis."[201] While leveraging commercial capabilities for military advantage is not new, it must happen within regulatory bounds. As former NASA administrator Jim Bridenstine notes, this ensures that no private monopoly exists that the "government is dependent on."[202] For, if commercial actors, with the tacit compliance of the government, get too much power, then governments will struggle to rein them in and ensure alignment of commercial interests with national ones.

E. CONCLUSION

The battlefield is changing. Wars have transcended traditional state-on-state conflict, with combatants no longer solely donning their nation's colors and fighting on the land or sea. Instead, they are fought in all domains and by a wide variety of individuals. Rapid technological advancement has permitted battlefield influence by non-state actors, organizations, and individuals at unprecedented levels. To that end, some assert that the "convergence of technological advances is leading to a revolution in military affairs."[203] These technological advancements complicate the battlefield as recent military technologies and capabilities have increasingly become highly indistinguishable and highly integrated compared to civilian counterparts. When the demarcation line between a civilian capability and a military one becomes increasingly thin, international tensions will naturally rise as states question the intentions of others.

[200] Satariano et al., "Elon Musk's Unmatched Power in the Stars."

[201] Courtney Albon, "Space Force Finalizes Plan for Commercial Surge Capacity during Crisis," Defense News, October 19, 2023, https://www.defensenews.com/battlefield-tech/space/2023/10/19/space-force-finalizes-plan-for-commercial-surge-capacity-during-crisis/.

[202] Farrow, "Elon Musk's Shadow Rule."

[203] Hammes, "The Tactical Defense Becomes Dominant Again," 10.

The 2022 U.S. National Defense Strategy recognizes the rapid evolution, noting that "fast-evolving technologies and applications are complicating escalation dynamics and creating new challenges for strategic stability."[204] While the line between a military and civilian asset has naturally thinned, it becomes even more troublesome when there is a deliberate intent to fuse the two together, resulting in complicated escalation dynamics and an uneasy future. This increasing entanglement becomes entrapment in areas of national security as it presents complications and dilemmas for the U.S. government. Deliberate co-mingling of capabilities results in detection, attribution, and optics dilemmas for the state wherein they may be in a perpetually disadvantaged position. Moreover, the civilian influence to encourage and commercially leverage this fusion only complicates matters as it obscures the traditionally held bounds of state action. While commercial influence is critical to further national interests and capabilities, policymakers must temper their complacency and ensure they drive international affairs, not private actors.

[204] Department of Defense, *National Defense Strategy of The United States of America*, 6.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSION

The rapid and deliberate fusion of dual-use technology amongst civilian and military sectors presents a worrisome trend. The distinction between civilian capabilities and their military counterparts continues to blur in an ever-connected world. This dilemma will be increasingly present in conflict worldwide, both in large-scale state-on-state action and operations that fall short of war. No longer is proximity to the battlefield, nor swearing an oath, a pre-requisite for wartime activity and engagement. Instead, every man, woman, and child…combatant and non-combatant alike, can wield weapons of war with disastrous consequences. No longer is it every soldier a rifleman, nor even "every soldier a sensor," but every person and every device a sensor, irrespective of who is in possession.[205]

The U.S. Army Training and Doctrine Command acknowledges this shift, wherein "traditional norms of warfare, definitions of combatants and non-combatants, and even what constitutes military action or national casus belli will be turned upside down."[206] This changing nature of international conflict presents unique challenges to traditional views on the ethics and morality of war according to the principles of just war theory. In addition, it also presents challenges to U.S. national security and dilemmas the U.S. is ill-prepared to handle. U.S. policymakers must acknowledge this shifting tide and adopt practices to reflect the incongruent reality of dual-use capabilities.

A. A NEW JUST WAR?

Modern Just War Theory analyzes wars and conflict via ethical and moral considerations. While some contend that there is a "shift in the ethics and law of warfare," this is simply untrue, as the ethics of war have not changed.[207] Instead, adapting and implementing new technologies and capabilities have lifted the fog of war in light of

[205] Stew Magnuson, "Army Wants to Make 'Every Soldier a Sensor,'" National Defense Magazine, May 1, 2007, https://www.nationaldefensemagazine.org/articles/2007/5/1/2007may-army-wants-to-make-every-soldier-a-sensor.

[206] U.S. Army Training and Doctrine Command, *The Operational Environment and the Changing Character of Warfare*, 23.

[207] U.S. Army Training and Doctrine Command, 23.

current practices. The ethics of right and wrong have not changed and must, therefore, be applied to recent struggles. Traditional JWT views break down wars amongst two lenses: *jus ad bellum*, the decision to go to war, and *just in bello*, just conduct in war.

Jus ad bellum generally addresses when nations are morally permissible to go to war. However, as mentioned previously, the notion of simple state-on-state conflict, with clear belligerents and battlefield fronts, is diminishing. Nonetheless, assessments shall be made that follow the intent of *jus ad bellum* to ensure that we do not enter into conflict unnecessarily or without due deliberation. Principles of *jus ad bellum* include a just cause with just intent, waged by a legitimate authority, a public declaration, proportionality, last resort, and a reasonable chance of success. However, the changing nature of the battlefield complicates the once-explicit differentiation of nation-states following these principles. Instead, it may permit non-state actors, commercial industry, or even individuals to employ wartime effects without adherence or consideration to *jus ad bellum* principles. This shift presents a dangerous opportunity where actors can engage with perceived impunity.

While *jus ad bellum* principles are concerned with the ethics of a nation going to war, *jus in bello* is concerned with the proper conduct of combatants engaged in war. Under this notion, the principles of proportionality and distinction are applied at the individual combatant and tactical level (vice national and strategic level, as in *jus ad bellum*). This difference portrays the possibility of just combatants waging an unjust war, unjust combatants waging a just war, or any combination thereof.

The *jus in bello* principle of proportionality concerns itself with the balance of good versus evil, wherein the military advantage foreseen from a particular action does not outweigh any expected civilian losses.[208] Additional Protocol I of the Geneva Conventions codifies this ethical principle of proportionality, where, throughout its text, it addresses the balance between civilian harm and military advantage. Proportionality in dual-use conflict is present as today's pivotal dual-use technology is highly integrated amongst military and civilian assets. For example, the same GPS satellite network that provides critical position,

[208] International Committee of the Red Cross, *International Humanitarian Law: Answers to Your Questions*, 47.

navigation, and timing data to the commercial industry is the same satellite network that provides GPS data to precision-guided munitions. An attack on this network would have widespread effects on the civilian population, which could even result in unnecessary and foreseen deaths. While an attack on the globally leveraged GPS satellite network represents an extremely acute threat, the convergence of dual-use capabilities and their integration amongst commercial and military sectors will increase, especially when there is a lack of distinction between the capabilities.

One of the oldest and most fundamental tenets of waging a just war is that belligerents will distinguish themselves from the civilian population. This deference was so distinct that civilians would often come to the battlefield as if going to the theater to watch a play, as they did in 1861 when they brought "along picnic baskets and opera glasses" to witness the Battle of Bull Run.[209] However, military assets, as well as civilians, have transitioned from being indirectly involved in a conflict to directly involved, and thus, pose critical questions of when a capability or person lost its protected status as a non-combatant and is, therefore, liable to attack. Warfare today sees both a deliberate and natural "intermingling of civilians with armed actors."[210] Renowned ICRC scholar, Kubo Mačák, acknowledges this intermingling and notes that this "contributes to the erosion of the principle of distinction."[211] Both the global community addresses this trend in the ICRC's Interpretive Guidance as well as within the U.S. in its DOD Law of War Manual.

Nonetheless, indistinct dual-use capabilities (e.g., Starlink satellites) and dual-use civilians (e.g., ones who provide direct and clear targeting information to military units) blur the line of combatant and continually present revolving door dilemmas. Even more troublesome is that many non-state actors rely on a nation's adherence to international laws and norms and intentionally conduct acts of perfidy as outlined in Article 37 of AP-1.[212]

[209] U.S. Senate, "U.S. Senate: Senators Witness the First Battle of Bull Run," accessed November 15, 2023, https://www.senate.gov/artandhistory/history/minute/Witness_Bull_Run.htm.

[210] Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 11.

[211] Mačák and Vignati, "Civilianization of Digital Operations."

[212] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 258.

While modern-day conflict may not see the perfidious extremes of feigning a white flag, multiple examples exist of attempts "with intent to betray" groups' adherence to customary laws of right and wrong.[213] The demarcation line between combatant and non-combatant, both in technology and persons, has become increasingly thin, and the problem is only exacerbated when there is a deliberate intermingling done on behalf of nation-states and non-state actors alike.

Traditional just war views hold that there is a distinction between *jus ad bellum* and *jus in bello*.[214] However, a revision is afoot, as the blurred lines between state actors, non-state actors, and civilian influence on the battlefield are changing the traditionally held views on a bifurcated *jus ad bellum* and *jus in bello.* The revisionist argument holds that the "permissibility of action in war cannot be divorced from the ends that the action serves."[215] This argument would then assert that individuals are morally liable for both *jus ad bellum* principles as well as *jus in bello*. This action-based liability removes the shield of membership and instead contends that non-state actors, commercial actors, and individuals shall be liable for their actions. The moral and ethical dilemmas in both the traditional and revisionist view are but one pillar of complications affecting U.S. adaptation to dual-use technology, the other being the security and stability of the United States.

B. THE NEW NORMAL?

Many challenges associated with dual-use objects and the ethical dilemma of distinction and proportionality also manifest in national security. Recent trends towards indistinguishable capabilities, which are highly integrated into the civilian and military society, affect U.S. national security, increasing the possibility of conflict and competition. The characteristics of distinguishability and integration lead to further security dilemmas in the form of deliberate co-mingling, detection issues, attribution dilemmas, and an optics narrative.

---

[213] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I), 258.

[214] Walzer, *Just and Unjust Wars*, 38.

[215] Jeff McMahan, "The Moral Responsibility of Volunteer Soldiers," Boston Review, October 28, 2013, https://www.bostonreview.net/forum/moral-wounds-ethics-volunteer-military-service/.

In the last few years, there has been an intentional movement to interweave military and civilian capabilities within the same asset. This fusion causes a distinguishability problem where an attacker does not quite know if the functionality of such capability is for peaceful or wartime purposes. Adversarial nations to the United States are leveraging this grey zone and, in turn, taking longstanding, highly distinguishable assets and manipulating them into dual-use capabilities. This problem is further complicated when an indistinguishable capability is woven deeply into civilian and military cultures.

While distinguishability reflects the ability of one to differentiate military from civilian applications, integration refers to how well-integrated a capability is to both civilian and military enterprises.[216] The more integrated a dual-use capability is into both sectors, the more difficult it will be to ascertain the true intended function of an asset. Furthermore, the more integrated it is, the more difficult it is to attack only the niche military application without affecting the civilian capability, and this integration and indistinguishability present security dilemmas for the United States.

Traditional deterrence does not work well when an adversary does not follow the prescribed norms or behavior, nor when the target of deterrence is not keenly aware of a capability. Traditionally, nuclear assets and conventional capabilities were intentionally separated as a means to isolate and contain the exquisite technology. However, recent trends have been to intentionally co-mingle traditional and nuclear assets in an attempt to protect both entities from attack. The logic therein is that states will not attack targets if there is a possibility of striking a nuclear target, thereby protecting both assets. Similarly, nations are now deliberately co-mingling civilian and military assets to obscure their true intentions and insulate them from potential harm.

This insulation, therefore, presents a detection dilemma for the United States where decision makers might not know the true intention of an asset until it is employed, and likely too late. While many technologies are developed for civilian use, their latent ability to rapidly transition into a military-supporting asset makes it inherently difficult to identify their intended use. Moreover, inherently dual-use technologies, with little to no latency,

[216] Vaynman and Volpe, "Dual Use Deception," 600.

such as space, cyber, and AI, blur the lines between benign and hostile applications as there is no way to detect the intent. By creating a detection dilemma, international agreements and norms aimed at governing and controlling the use of these assets will be difficult to obtain.

While a detection dilemma deals with *how* a dual-use capability will be employed, the attribution dilemma deals with *whom.* Attributing aggressive behaviors to state actors that have leveraged proxies or other loose affiliations is no new task. However, the subtle and nuanced nature of employment enjoyed by many dual-use capabilities and the ability to influence a campaign at the non-state actor level makes it difficult for response options on behalf of any aggrieved state. This lack of attribution, in terms of employment and origination, creates loopholes that can be exploited by our adversaries and, therefore, cause a security problem.

The last dilemma, optics, deals with how a dual-use capability is perceived by public perception. Unfortunately, many of the new dual-use technologies fielded today are misrepresented by states regarding their true nature and endgame usage. This problem is especially problematic when a perceived civilian capability is exposed as dual-use. This exposure could lead to a diplomatic quagmire, where one side tries to maintain its civilian implausibility, and the other challenges it, asserting that the capability will conduct military or covert action. Furthermore, the optics dilemma manifests in the international community's response and perception. Accusing a nation-state of maliciously leveraging benign dual-use objects without irrefutable evidence (or intelligence that a state is willing to disclose) can strain international relations and result in accusations of complicity or undue hostility. Conversely, failure to address such concerns emboldens states to continue or escalate these activities while continuing to present a security threat.

These dilemmas and security issues have primarily been viewed through the lens of state-on-state actors. However, the pervasiveness of dual-use capabilities is no longer enjoyed at only national levels. Instead, dual-use capabilities present issues in individual support and culpability as non-state actors, commercial actors, and individuals alike leverage this technology. Leveraging technology below the statehood level could result in an unawareness of the user and the capability regarding the danger they may be

inadvertently subjecting themselves to, a garnering of power and influence that could rival nation-states, and injecting themselves into a conflict for which the government cannot control or oversee their actions. The increasing civilianization of the battlefield will only expand as the military's dependence on dual-use capabilities increases and thus presents a daunting reality where civilian influence on the battlefield eclipses that of state governments.

Dual-use technology and capability usage will continue expanding, becoming more integrated and indistinguishable, thereby rendering what constitutes a legitimate military target under traditional JWT theory cumbersome. While this thesis set out to identify a framework to identify dual-use capabilities and when a threshold for targeting has been, like most aspects of law, there is no prescriptive checklist that will lead to a morally right or wrong answer. The result, instead, is an awareness of the complications associated with dual-use technology and an appreciation for how its use will increase competition and shape the battlefield. As there is no longer a natural dual-use flow of technology but a deliberate attempt to make it indistinguishable, one can expect a new variant of an arms race and increased competition. However, instead of overt arms racing, one will see covert pursuit and unclear aims and objectives. Not only will this affect the threshold of competition, but it will also shape the incentives for going to war.

Some may argue that dual-use technology and capabilities will provide stabilizing effects on the international community. If commercial and military capabilities are intertwined and integrated, then perhaps the fear of inadvertent escalation is too great to overcome and thus results in a stalemate. In addition, a stabilizing benefit of dual-use technology is that it leverages an efficient use of resources and drives tech advancements. Lastly, it could enhance national security by promoting innovation and economic growth. This stabilizing effect is idealistic, and unlikely to be achieved due to many actors with different intentions and desired outcomes.

The more likely effect of dual-use technology is that it will result in destabilizing consequences for the international community. Continually blurred lines will lead to increased militarization of civilian spaces and thereby lead to an arms race as nations seek to out-compete one another under the guise of civilian technology. This ruse will only

deepen the distinguishability and integration that is already plaguing dual-use technology. In addition, worldwide integration will make it easier for non-state actors and individuals to acquire and leverage capabilities, thereby influencing the world order at a personal, acute, level. This capability represents a worrisome trend that U.S. policymakers must address regarding offensive and defensive operations.

C. RECOMMENDATIONS

State actors have traditionally been held liable (under *jus ad bellum*) for going to war. However, new technologies and capabilities may permit non-state actors, corporations, or even individuals to have power that eclipses that of many governments. For this reason, a reevaluation should be conducted to identify culpability for wartime and warlike actions. The concept of a legal and lawful combatant needs to be expanded beyond those in traditional military uniforms to encompass those who play active roles in conflicts, even from remote locations or through technical means. Jeff McMahan acknowledges this revisionist argument and asserts that "the permissibility of action in war cannot be divorced from the ends that the action serves."[217] There should no longer be a simple jus ad bellum distinction that applies to organizations/nations and a different set of rules jus in bello that apply to individuals; the same principles must be used at the individual level to address the changing nature of war and who is culpable.

In addition to reevaluating the ethics and just action of combatants in war, the U.S. military needs to address the changing trend of warfare and what is targetable under international law. Customary international law and international agreements take years to craft and will always be a lagging indicator of right and wrong. Furthermore, the law sets a minimum legal baseline, and the U.S. needs to identify its moral baseline regarding targeting dual-use technology and capabilities. Commanders will be forced to make these difficult decisions on the battlefield, where they need to identify the issue and realize the optics of their actions. For this reason, the U.S. military needs to incorporate dual-use targets and technology into its exercises and drills to provide commanders insight and

[217] McMahan, "The Moral Responsibility of Volunteer Soldiers."

lessons learned into the nuance of dual-use targets and objectives in operations that fall short of armed conflict.

In addition to exercises and drills, the U.S. must protect itself from vulnerabilities by leveraging dual-use capabilities. The current budgetary and appropriations process results in unpredictability for new initiatives and stymies innovation.[218] As a result, the military often looks to circumvent the process and instead pursue a commercial option. Former Secretary of Defense, Robert Gates, acknowledges that the Pentagon "must fix its sclerotic, parochial, and bureaucratic acquisition process, which are especially anachronistic in an era when agility, flexibility, and speed matter more than ever."[219] This change is critical to protect critical U.S. infrastructure and ensure that commercial support to the military is leveraged in a secure manner. White House National Security Advisor, Jake Sullivan, notes the importance of protecting sensitive technologies by creating a "small yard and a high fence."[220] Under this principle, the U.S. needs to be very prescriptive regarding its openness to new technologies and how it handles innovation. The U.S. can achieve a strategic balance in leveraging commercial and militarized dual-use technology by implementing robust safeguards that bolster national security. This balance will simultaneously "supporting an interconnected global economy," ensuring that new advancements do not compromise national security nor create undue vulnerabilities.

The dual-use dilemma is not restricted to difficulties facing the United States, but is instead a global dilemma where international laws and norms need to reflect the reality of non-combatant influence in conflict. Protection for civilians has always been, and should continue to be, one of the core tenets of just war. However, their protection is not absolute, and current laws and norms offer broad protection and latitude for nefarious action. Accountability and culpability need to reflect modern war, where the power of one can significantly influence the battlespace. The principles of Just War Theory are just as

[218] Robert Gates, "The Dysfunctional Superpower," *Foreign Affairs*, September 29, 2023, https://www.foreignaffairs.com/united-states/robert-gates-america-china-russia-dysfunctional-superpower.

[219] Gates.

[220] Jake Sullivan, "The Sources of American Power," *Foreign Affairs*, October 24, 2023, https://www.foreignaffairs.com/united-states/sources-american-power-biden-jake-sullivan.

important today, where fighting justly is of the utmost importance. War and conflict are not going away; instead, the threshold for what constitutes armed conflict is eroding, thus precariously placing the ethics of right and wrong in a difficult position. However, the intent remains the same, and as Friedrich Nietzsche noted, "he who fights with monsters should look to it that he himself does not become a monster."[221] Dual-use technology presents significant global benefits, yet it is imperative to carefully navigate its inherent risks, including international tension, escalation, and the challenges of culpability and non-combatant immunity. The international community needs to, as the London Tube reminds us, *mind the gap* regarding dual-use technology before the doors close and opportunities for peaceful leveraging of dual-use capabilities are irrevocably compromised.

[221] Friedrich Nietzsche, *Beyond Good and Evil*, trans. Helen Zimmern, The Complete Works of Friedrich Nietzsche (1909-1913) (London: T.N. Foulis, 1909), 97.

LIST OF REFERENCES

Acton, James. "Summary." In *Entanglement: Chinese and Russian Perspectives on Non-Nuclear Weapons and Nuclear Risks*, edited by James Acton, 1–7. Washington, DC: Carnegie Endowment for International Peace, 2017. https://carnegieendowment.org/2017/11/08/underappreciated-risks-of-entanglement-chinese-perspective-pub-73164.

Air Force Research Laboratory. "Rapid Dragon." Wright-Patterson Air Force Base, OH: Air Force Research Laboratory, 2022. https://afresearchlab.com/wp-content/uploads/2021/09/AFRL_Rapid-Dragon_FS_0122.pdf.

Albon, Courtney. "Space Force Finalizes Plan for Commercial Surge Capacity during Crisis." Defense News, October 19, 2023. https://www.defensenews.com/battlefield-tech/space/2023/10/19/space-force-finalizes-plan-for-commercial-surge-capacity-during-crisis/.

The ALS Group. "6 Cyber Attacks That Caused Property Damage." The ALS Group, March 14, 2017. https://info.thealsgroup.com/blog/cyber-attacks-property-damage.

Aquinas, Thomas. *Summa Theologica, Part II-II*. Salt Lake City, Utah: Project Gutenberg, 2006. https://www.gutenberg.org/ebooks/18755.

Austin, Lloyd. "Statement From Secretary of Defense Lloyd J. Austin III." Department of Defense, February 4, 2023. https://www.defense.gov/News/Releases/Release/Article/3288535/statement-from-secretary-of-defense-lloyd-j-austin-iii/#:~:text=The%20balloon%2C%20which%20was%20being,down%20above%20U.S.%20territorial%20waters.

Beard, Jack. "The Principle of Proportionality in an Era of High Technology." In *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, edited by Christopher Ford and Winston Williams, 261–88. New York, NY: Oxford University Press, 2019.

Becker, Tom. "Guns and Butter 2.0." BlackRock, March 8, 2023. https://www.blackrock.com/us/individual/insights/guns-and-butter.

Biden, Joseph. *National Security Strategy of the United States of America*. Washington, DC: White House, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

Bingen, Kari, Kaitlyn Johnson, and Makena Young. "Space Threat Assessment 2023." Washington, DC: Center for Strategic and International Studies, April 2023. https://www.csis.org/analysis/space-threat-assessment-2023.

Brunstetter, Daniel. "The Decision to Use Military Force in Recent Moral Argument." In *The Ashgate Research Companion to Military Ethics*, edited by James Johnson and Eric Patterson, 25–37. New York: Routledge, 2015.

Carus, W. Seth. "A Century of Biological-Weapons Programs (1915–2015): Reviewing the Evidence." *The Nonproliferation Review* 24, no. 1–2 (January 2017): 129–53. https://doi.org/10.1080/10736700.2017.1385765.

Chyba, Christopher F. "New Technologies & Strategic Stability." *Daedalus* 149, no. 2 (April 2020): 150–70. https://doi.org/10.1162/daed_a_01795.

Clark, Stephen. "NRO Reveals Plans for Previously Undisclosed SpaceX Launch This Month." Spaceflight Now, October 5, 2020. https://spaceflightnow.com/2020/10/05/nro-reveals-plans-for-previously-undisclosed-launch-with-spacex-this-month/.

Cook, Martin. "The Role of the Military in the Decision to Use Armed Force." In *The Ashgate Research Companion to Military Ethics*, edited by James Johnson and Eric Patterson, 49–58. New York: Routledge, 2016.

Council on Foreign Relations. "Stuxnet." New York: Council on Foreign Relations, July 2010. https://www.cfr.org/cyber-operations/stuxnet.

Day, Dwane. "Nuking Moscow with a Space Shuttle." The Space Review, December 23, 2019. https://www.thespacereview.com/article/3855/1.

Demerly, Tom. "The Aviationist: 73 Years Ago Today: The Deadliest Air Raid in History, Operation Meetinghouse." Newstex, March 9, 2018. https://www.proquest.com/docview/2012144060/citation/A8DF2CFD58284FBDPQ/1.

Department of Defense. "Abu Musab Al-Zarqaw Dead." Department of Defense, June 8, 2006. https://www.defense.gov/Multimedia/Photos/igphoto/2001967287/.

Department of Defense. *Law of War Manual*. Washington, DC: Department of Defense, 2023. https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF.

Department of Defense. *National Defense Strategy of The United States of America*. Washington, DC: Department of Defense, 2022. https://apps.dtic.mil/sti/trecms/pdf/AD1183539.pdf.

Department of State. "The Chinese Communist Party's Military-Civil Fusion Policy." Department of State. Accessed February 5, 2023. https://2017-2021.state.gov/military-civil-fusion/.

Euractiv. “Crimea Bridge Is Legitimate Military Target, Zelenskyy Says.” Euractiv, July 22, 2023. https://www.euractiv.com/section/global-europe/news/crimea-bridge-is-legitimate-military-target-zelenskyy-says/.

European Commission. “Exporting Dual-Use Items.” European Commission, January 27, 2023. https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en.

European Commission. “Report from the Commission to the European Parliament and the Council: Mid-Term Review of the European Satellite Radio Navigation Programmes.” Brussels: European Commission, 2011. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0005:FIN:EN:PDF.

Farrow, Ronan. “Elon Musk’s Shadow Rule.” *The New Yorker*, August 21, 2023. https://www.newyorker.com/magazine/2023/08/28/elon-musks-shadow-rule.

Federal Aviation Administration. *Airspace Designations and Reporting Points*. JO 7400.11H. Washington, DC: Federal Aviation Administration, 2023. https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1038054.

Foltz, Andrew. “Stuxnet, Schmitt Analysis, and the Cyber ‘Use-of-Force’ Debate.” *Joint Forces Quarterly* 4th Quarter, no. 67 (2012): 40–48. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf.

Gallaher, Michael. “Economic Benefits of the Global Positioning System.” Presented at the Positioning, Navigation and Timing Advisory Board Meeting, November 20, 2019. https://www.gps.gov/governance/advisory/meetings/2019-11/gallaher.pdf.

Garamone, Jim. “F-22 Safely Shoots Down Chinese Spy Balloon Off South Carolina Coast.” U.S. Department of Defense, February 4, 2023. https://www.defense.gov/News/News-Stories/Article/Article/3288543/f-22-safely-shoots-down-chinese-spy-balloon-off-south-carolina-coast/.

Gates, Robert. “The Dysfunctional Superpower.” *Foreign Affairs*, September 29, 2023. https://www.foreignaffairs.com/united-states/robert-gates-america-china-russia-dysfunctional-superpower.

Global Security. “3M-54 Klub.” Global Security. Accessed November 1, 2023. https://www.globalsecurity.org/military/world/russia/club.htm.

Hallgarth, Matthew. “Just War Theory and Remote Military Technology: A Primer.” In *Killing by Remote Control*, edited by Bradley Strawser, 25–46. New York: Oxford University Press, 2013.

Hammes, T.X. “The Tactical Defense Becomes Dominant Again.” *Joint Forces Quarterly* 103, no. 4 (2021): 10–17. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2807244/the-tactical-defense-becomes-dominant-again/.

International Committee of the Red Cross. “Direct Participation in Hostilities: Questions & Answers.” February 6, 2009. https://www.icrc.org/en/doc/resources/documents/faq/direct-participation-ihl-faq-020609.htm.

International Committee of the Red Cross. *International Humanitarian Law: Answers to Your Questions*. Geneva: International Committee of the Red Cross, 2023. https://shop.icrc.org/international-humanitarian-law-answers-to-your-questions-pdf-en.html.

International Committee of the Red Cross. “Jus Ad Bellum and Jus in Bello.” October 29, 2010. https://www.icrc.org/en/document/jus-ad-bellum-jus-in-bello.

Isaacson, Walter. *Elon Musk*. New York: Simon & Schuster, 2023.

Kessler, Donald J., and Burton G. Cour-Palais. “Collision Frequency of Artificial Satellites: The Creation of a Debris Belt.” *Journal of Geophysical Research: Space Physics* 83, no. A6 (June 1978): 2637–46. https://doi.org/10.1029/JA083iA06p02637.

King, Matthew. “High-Tech Civilians, Participation in Hostilities, and Criminal Liability.” In *The Impact of Emerging Technologies on the Law of Armed Conflict*, edited by Ronald Alcala and Eric Jensen, 175–76. New York: Oxford University Press, 2019.

Mabeus, Courtney. “Chinese Navy Using Commercial Car Ferries to Launch Amphibious Landing Craft.” USNI News, July 26, 2021. https://news.usni.org/2021/07/26/chinese-navy-using-commercial-car-ferries-to-launch-amphibious-landing-craft.

Mačák, Kubo, and Mauro Vignati. “Civilianization of Digital Operations: A Risky Trend.” Lawfare, April 5, 2023. https://www.lawfaremedia.org/article/civilianization-digital-operations-risky-trend.

Magnuson, Stew. “Army Wants to Make ‘Every Soldier a Sensor.’” *National Defense Magazine*, May 1, 2007. https://www.nationaldefensemagazine.org/articles/2007/5/1/2007may-army-wants-to-make-every-soldier-a-sensor.

Mahfoud, Tara, Christine Aicardi, Saheli Datta, and Nikolas Rose. “The Limits of Dual Use.” *Issues in Science and Technology* 34, no. 4 (Summer 2018). https://issues.org/the-limits-of-dual-use/.

Maroonian, Anaïs. “Proportionality in International Humanitarian Law: A Principle and a Rule.” *Lieber Institute West Point*, October 24, 2022. https://lieber.westpoint.edu/proportionality-international-humanitarian-law-principle-rule/.

Marquardt, Alex. "Exclusive: Musk's SpaceX Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick up the Tab." CNN, October 14, 2022. https://www.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.

McMahan, Jeff. "Just Cause for War." *Ethics & International Affairs* 19, no. 3 (December 2005): 1–21. https://doi.org/10.1111/j.1747-7093.2005.tb00551.x.

McMahan, Jeff. *Killing in War*. Oxford: Oxford University Press, 2011.

McMahan, Jeff. "The Moral Responsibility of Volunteer Soldiers." Boston Review, October 28, 2013. https://www.bostonreview.net/forum/moral-wounds-ethics-volunteer-military-service/.

Melzer, Nils. *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law.* Geneva: International Committee of the Red Cross, 2009.

Merlin, Peter. "Design and Development of the Blackbird: Challenges and Lessons Learned." In *47th AIAA Aerospace Sciences Meeting*. Orlando, FL: American Institute of Aeronautics and Astronautics, 2009. https://doi.org/10.2514/6.2009-1522.

Ministry of Foreign Affairs of the People's Republic of China. "Statement on the U.S. Claim of Shooting Down the Chinese Unmanned Airship." February 5, 2023. https://www.mfa.gov.cn/zyxw/202302/t20230205_11019861.shtml.

Ministry of Foreign Affairs of Ukraine. "15-Year-Old Andrii Helped Destroy a Column of Russian Equipment Thanks to His Drone Skills." June 2022. https://war.ukraine.ua/heroes/15-year-old-andrii-helped-destroy-a-column-of-russian-equipment-thanks-to-his-drone-skills/.

Moscufo, Michela. "'Drone Boy' Becomes Hero in Ukraine after Taking out a Line of Russian Tanks." ABC News, August 2022. https://abcnews.go.com/International/drone-boy-hero-ukraine-taking-line-russian-tanks/story?id=88740689.

Morris, Errol, dir. *The Fog of War*. 2003; Los Angeles, CA: Sony Pictures Classics, 2003. https://tv.apple.com/us/movie/the-fog-of-war/umc.cmc.3j815y9s5id2nvfztrlfh75il.

Moseley, Alexander. "Just War Theory." Internet Encyclopedia of Philosophy at the University of Tennessee at Martin. Accessed November 21, 2023. https://iep.utm.edu/justwar/.

Muñoz-Rojas, Daniel, and Jean-Jacques Frésard. "The Roots of Behaviour in War: Understanding and Preventing IHL Violations." *International Review of the Red Cross* 86, no. 853 (March 2004): 189–206. https://doi.org/10.1017/S1560775500180150.

National Museum of American History. "Ball Bearing." Accessed February 5, 2023. https://americanhistory.si.edu/collections/search/object/nmah_846532.

Niccol, Andrew, dir. *Lord of War*. 2005; Santa Monica, CA: Lions Gate Films, 2005. http://www.video.amazon.com

Nietzsche, Friedrich. *Beyond Good and Evil*. Translated by Helen Zimmern. The Complete Works of Friedrich Nietzsche (1909-1913). London: T.N. Foulis, 1909.

O'Brien, William Vincent. *The Conduct of Just and Limited War*. New York, N.Y: Praeger, 1981.

Orend, Brian. "Jus Post Bellum: The Perspective of a Just-War Theorist." *Leiden Journal of International Law* 20, no. 3 (September 2007): 571–91. https://doi.org/10.1017/S0922156507004268.

Quinn, Dale. "Venezuela Condemns U.S. for Shooting Down Chinese Balloon." *Bloomberg*, February 5, 2023. https://www.bloomberg.com/news/articles/2023-02-05/venezuela-condemns-us-for-shooting-down-chinese-balloon.

Rizer, Kenneth R. "Bombing Dual-Use Targets: Legal, Ethical, and Doctrinal Perspectives." *Air and Space Power Journal*, May 2001. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/Rizer.pdf.

Rogoway, Tyler. "Northrop Grumman Shows Off Shipping Container-Launched Anti-Radiation Missile Concept." The Drive, October 8, 2018. https://www.thedrive.com/the-war-zone/24111/northrop-grumman-shows-off-shipping-container-launched-anti-radiation-missile-concept.

Roscini, Marco. "World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force." In *Max Planck Yearbook of United Nations Law*, edited by Armin von Bogdandy and Rudiger Wolfrum, 14:85–130. Leiden, NL: Brill, 2010. https://brill.com/view/journals/mpyo/14/1/article-p85_4.xml.

Sari, Aurel. "Hybrid Warfare, Law, and the Fulda Gap." In *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, edited by Christopher Ford and Winston Williams, 161–90. New York: Oxford University Press, 2018.

Satariano, Adam, Scott Reinhard, Cade Metz, Sheera Frenkel, and Malika Khurana. "Elon Musk's Unmatched Power in the Stars." *The New York Times*, July 28, 2023. https://www.nytimes.com/interactive/2023/07/28/business/starlink.html.

Schmid, Stefka, Thea Riebe, and Christian Reuter. "Dual-Use and Trustworthy? A Mixed Methods Analysis of AI Diffusion Between Civilian and Defense R&D." *Science and Engineering Ethics* 28, no. 2 (April 2022): 1–23. https://doi.org/10.1007/s11948-022-00364-7.

Schmitt, Michael, and Liis Vihul, eds. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

St. Augustine. "Letter 189." New Advent, 418AD. https://www.newadvent.org/fathers/1102189.htm.

Stoddard, Catherine. "15-Year-Old Ukrainian Boy Dubbed a Hero after Using Drone to Help Defeat Russian Forces." Fox 32 Chicago, June 8, 2022. https://www.fox32chicago.com/news/15-year-old-ukrainian-boy-dubbed-a-hero-after-using-drone-to-help-defeat-russian-forces-report.

Stowsky, Jay. "Secrets to Shield or Share? New Dilemmas for Military R&D Policy in the Digital Age." *Research Policy* 33, no. 2 (March 2004): 257–69. https://doi.org/10.1016/j.respol.2003.07.002.

Sullivan, Jake. "The Sources of American Power." *Foreign Affairs*, October 24, 2023. https://www.foreignaffairs.com/united-states/sources-american-power-biden-jake-sullivan.

U.S. Air Force. "Special Reconnaissance." Accessed October 16, 2023. https://www.airforce.com/careers/combat-and-warfare/special-warfare/special-reconnaissance.

U.S. Army Training and Doctrine Command. *The Operational Environment and the Changing Character of Warfare*. Fort Eustis, VA: Department of the Army, 2019.

U.S. Senate. "U.S. Senate: Senators Witness the First Battle of Bull Run." Accessed November 15, 2023. https://www.senate.gov/artandhistory/history/minute/Witness_Bull_Run.htm.

Vaynman, Jane, and Tristan A. Volpe. "Dual Use Deception: How Technology Shapes Cooperation in International Relations." *International Organization* 77, no. 3 (September 2023): 599–632. https://doi.org/10.1017/S0020818323000140.

Walzer, Michael. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. New York: Basic Books, 2006.

Waxman, Matthew. *International Law and the Politics of Urban Air Operations*. Santa Monica, CA: Rand, 2000. https://doi.org/10.7249/MR1175.

Wessner, Charles, and Sujai Shivakumar. *Renew SBIR, Just Defend the Recipients against China*. Washington, DC: Center for Strategic & International Studies, 2022. https://www.csis.org/analysis/renew-sbir-just-defend-recipients-against-china.

White, Sarah. "Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine." PhD Diss., Harvard, 2019. https://dash.harvard.edu/handle/1/42013038.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California