UVU SECURITY REVIEW

Volume I
Issue 1
Spring 2020

UVU SECURITY REVIEW

ISSN 2576-1595

Center for National Security Studies
Utah Valley University
800 West University Parkway
Orem, UT 84058

www.uvu.edu/nss/journal.html

UVU SECURITY REVIEW

VOLUME IV SPRING 2020 ISSUE 1A

UVU SECURITY REVIEW

The *UVU Security Review* is Utah's first student-edited academic journal focused on national security issues. The journal is published twice annually—in April and December—and it is supported by the Center for National Security Studies (CNSS) at Utah Valley University (UVU). The *Review* publishes timely, insightful articles on critical national security matters, including topics relating to foreign affairs, intelligence, homeland security, terrorism, and national defense. The *UVU Security Review* accepts articles from UVU students, alumni, faculty, staff, and administration. Submissions should be sent to the Editor-in-Chief at nationalsecurity@uvu.edu.

The Center for National Security Studies

The CNSS at UVU was established in January 2016. The Center is the first of its kind in the State of Utah. The CNSS is a nonpartisan academic institution for the instruction, analysis, and discussion of issues related to the field of US national security. The mission of the CNSS is twofold: to promote an interdisciplinary academic environment on campus that critically examines both the theoretical and practical aspects of national security policy and practice; and to assist students in preparing for public and private sector national security careers through acquisition of subject matter expertise, analytical skills, and practical experience. The CNSS aims to provide students with the knowledge, skills, and opportunities needed to succeed in the growing national security sector.

Utah Valley University

UVU is a teaching institution that provides opportunity, promotes student success, and meets regional educational needs. UVU builds on a foundation of substantive scholarly and creative work to foster engaged learning. The university prepares professionally competent people of integrity who, as lifelong learners and leaders, serve as stewards of a globally interdependent community.

CONTENTS

A Note from the Editor-in-Chief

Samuel D. Elzinga

I have thought long and hard what to say as editor-in-chief of this edition of this journal. What began as a normal semester both academically and for the journal quickly shifted to a format foreign to many, universally altering how we went about our lives. Students across the country traded backpacks for masks and classroom desks for dining room tables. It goes without saying that this pandemic has impacted the world severely. This is a time of confusion for many, as well as a time where it seems that all hope is lost. I cannot speak for many things beyond this journal, but I hope that the publication of this highlights the coming return to normalcy.

This is the first edition of the fourth year of this journal. For four years every fall and spring semester, a dedicated group of students on UVU's campus worked tirelessly to produce this edition of the journal, as well as help bring into creation a new forum for scholarly work on national security: our first online publication titled the *UVU Security Review*. This journal will be published once a year in the spring, highlighting work specifically from UVU students. As our flagship publication, the *UVU Journal of National Security*, continues to grow, we find it fitting to continue to provide an outlet just for UVU students to publish their work.

I could not thank Dr. Gregory Jackson and Mr. Ryan Vogel for their mentorship helping expand the journal to include more graduate school submissions this semester, as well as my dedicated Executive Editor, Hannah Lewis. I would like to thank my managing editors, Cierra Peters and Cougar Einfeldt, for their help, as well as my team of twelve content editors for their work on the journal. Additionally, this journal would not be the caliber it is without the support from Dr.

Deb Thornton and her dedicated editing class. Lastly, I would like to thank Deputy Assistant Secretary of State Mr. John Dinkelman for his forward and Professor Mary Kent for her faculty contribution. This journal, like many things in life, is a team effort, and I would not trade it for the world. It is my sincere wish you would enjoy this edition of the journal and welcome it as a refuge from our self-isolated lives.

Samuel Elzinga
Editor-in-Chief
UVU Journal of National Security

Ethics and Legalities of Artificial Intelligence and Lethal Autonomous Weapons in Warfare

Alyson Hatch

In our society, technological developments are constantly increasing, and the cyber world is quickly becoming more prominent than ever in many aspects of our lives. Much like the "space race" during the Cold War, nations, including the United States, are racing to be the first to develop ground-breaking technology, including artificial intelligence (AI) and advanced lethal autonomous weapons. This paper will discuss current laws surrounding artificial intelligence and lethal autonomous weapons, ethics of war and artificial intelligence, regulations that should be put into place governing the use of AI and lethal autonomous weapons in warfare, and the future of warfare with the use of AI. With continuous discoveries and developments on the cyber front, it is imperative that restrictions and regulations are put in place to uphold the ethical use of these new developments in warfare.

Currently, the United States is confronting technological advancements from countries such as Russia and China. China is becoming a cyber powerhouse. With recent technological developments, such as China's establishment of 5G networks,[1] China poses a major concern for the United States. It is feared that the Chinese will continue to develop technology that, if perfected, would be detrimental in the wrong hands. According to an article released by The White House Office of Trade and Manufacturing Policy, titled "How China's Economic Aggression Threatens the Technologies and Intellectual Properties of the United States and the World," the United States identifies two categories of economic aggression that China focuses on: "acquire key technologies and intellectual property from other countries, including the

1. Stu Woo, "In the Race to Dominate 5G, China Sprints Ahead," *The Wall Street Journal*, September 7, 2019, https://www.wsj.com/articles/in-the-race-to-dominate-5g-china-has-an-edge-11567828888.

United States, and capture the emerging high-technology industries that will drive future economic growth and many advancements in the defense industry."[2] China does not adhere to international rules and norms, and given the fact that artificial intelligence and lethal autonomous weapons systems are still new territory, it can be expected that China will use whatever means necessary to get ahead in the race and become the global technological superpower. In fact, China is already surpassing the United States in many aspects of artificial intelligence. According to a CNBC article by Frederick Kempe, "By the end of 2017, Chinese venture capital investors had poured enough into AI startups that they made up 48 percent of all AI venture funding globally, surpassing the US for the first time."[3] The Chinese are quickly approaching becoming the global technological superpower. As stated in the US–China Economic and Security Review Commission, "The Chinese government is implementing a comprehensive, long-term industrial strategy to ensure its global dominance."[4]

Because the development of such technology is so unpredictable, many law and policy makers debate how to regulate the use of AI and lethal autonomous weapons, specifically in the federal government. Some of the main issues facing lethal autonomous weapon systems (LAWS) in warfare are "distinction and proportionality."[5] One military technique designed to assist in decision making was the OODA loop, which stands for "observe-orient-decide-act." This technique was implemented into warfare by Air Force Colonel John Boyd and is used to train combatants to use discretion when making tactical or operational

2. White House Office of Trade and Manufacturing Policy, "How China's Economic Aggression Threatens the Technologies and Intellectual Properties of the United States and the World," *White House Office of Trade and Manufacturing Policy*, June 2, 2018, https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.

3. Frederick Kempe, "The US Is Falling Behind China in Crucial Race for AI Dominance," *CNBC*, January 25, 2019, https://www.cnbc.com/2019/01/25/chinas-upper-hand-in-ai-race-could-be-a-devastating-blow-to-the-west.html.

4. US–China Economic and Security Commission, 2017 Report to Congress, 24, US Government Publishing Office, November 2017, https://www.uscc.gov/sites/default/files/annual_reports/2017_Annual_Report_to_Congress.pdf.

5. Executive Office of the President, National Science and Technology Council and Committee on Technology, "Preparing for the Future of Artificial Intelligence," *The Office of Science and Technology Policy*, 38, October 12, 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

decisions on the spot.[6]

The question we face is how to train autonomous systems and AI to react in a way that successfully uses the OODA loop to distinguish between civilians and combatants. The purpose of using LAWS and AI in warfare is to distance human beings from the carnage of war as much as possible. Their use would make it safer for the combatant and allow for more precision in targeting and eliminating the enemy.[7]

The International Committee of the Red Cross (ICRC) has outlined laws that are currently in place regarding employment of new weapons. These laws are acknowledged and accepted by most countries, including the United States. The new weapon must adhere to the following criteria:

> First, are the new weapons prohibited by specific international conventions, such as the Chemical Weapons Convention, Biological Weapons Convention or Convention on Certain Conventional Weapons? Second, would such weapons cause superfluous injury or unnecessary suffering, or widespread, long-term and severe damage to the natural environment (Art 35 API)? Third, will such weapons likely have the effects of indiscriminate attacks (Art 51 API)? Lastly, will such weapons accord with the principles of humanity and dictates of public conscience—the Martens Clause (Art 1(2) API)?[8]

Necessity and whether or not it is humane are very important points to consider in the employment of a new weapon. Will the weapon make certain tasks and operations easier and quicker? Does the weapon reasonably limit suffering?[9] The purpose of warfare is not to cause unnecessary and extreme suffering but to quickly and efficiently eliminate enemy threats. Laws and regulations will continue to adjust to fit the growing autonomous warfare industry, but as of now, while

6. Steve Papenfuhs, "The OODA Loop, Reaction Time, and Decision Making," *Lexipol*, February 23, 2012, https://www.policeone.com/use-of-force/articles/the-ooda-loop-reaction-time-anddecision-making-fEOcXtsXFutU07cY/.

7. Executive Office of the President, "Preparing for the Future."

8. Qiang Li and Dan Xie, "Legal Regulation of AI Weapons Under International Humanitarian Law: A Chinese Perspective," *ICRC Blog*, May 2, 2019, https://blogs.icrc.org/lawand-policy/2019/05/02/ai-weapon-ihl-legal-regulation-chinese-perspective/.

9. Li and Xie, "Legal Regulation of AI Weapons."

many aspects of this field are still untested and unfamiliar, it is best to use current policies as guidelines for how to parse this tricky subject. Directive No. 3000.09 released by the Department of Defense provides guidelines for developing/deploying autonomous weapons. They require that these autonomous weapons go through extensive testing in order to ensure their capabilities and functions in real life scenarios.[10] Another DoD Directive, No. 5000.01, outlines the purpose and goal of the Defense Acquisition System: "The Defense Acquisition System exists to manage the nation's investments in technologies, programs, and product support necessary to achieve the National Security Strategy and support the United States Armed Forces."[11] Furthermore, it discusses policies on flexibility, responsiveness, innovation, discipline, and streamlined and effective management. These guidelines/goals govern the development and use of present and future technology in warfare. The policies are in place to ensure that new technologies meet the needs of the military and are used to advance US operational initiatives.[12]

Ethics are crucial to keep in mind when discussing warfare and international humanitarian law, and ethics cannot be cast aside in the consideration of LAWS and AI. Machines, no matter how "smart" or how intricately programmed, are still just that: machines. They do not have human emotions, morals, or values and therefore cannot show mercy or think through complicated situations regarding humane or inhumane acts.[13]

However, in order to understand the ethics of AI and LAWS on the battlefield, one must first understand the ethics of warfare. In a War College podcast titled "Ethical Behavior on the Battlefield," philosophy professor Pauline Kaurin discusses the ethics of warfare with Matthew Gault. She says war in and of itself is not a moral, ethical act; however, in certain circumstances when war is inevitable, there are justifications for otherwise unethical behavior. Ethics and morality during wartime set boundaries and laws to regulate how combatants behave in

10. Department of Defense, "Directive No. 3000.09," *The Defense Acquisition System*, November 21, 2012. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf.

11. Department of Defense, "Directive No. 5000.01." *The Defense Acquisition System*, May 12, 2003. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf.

12. Department of Defense, "Directive No. 5000.01."

13. Li and Xie, "Legal Regulation of AI Weapons."

order to minimize suffering.[14] One of the concerns regarding ethics in LAWS and AI is the claim that such technology would "dehumanize" warfare.[15] Some believe using technology to increase precision in targeting enemies and physically removing the human from war will significantly decrease combatant casualties. Others disagree, claiming that death by a robot strips the victim of respect and dignity.[16] In a Future of Life Institute podcast titled "Law and Ethics of Artificial Intelligence," Matt Scherer and Ryan Jenkins discuss with Ariel Conn the ethical and legal issues that are raised when it comes to autonomous weapons and artificial intelligence in general. They state that "law does not move as fast as technology does."[17] With the fast-paced rate that technology is growing and developing, ethics and law struggle to keep up. While helpful policies are in place, it is difficult to predict the future of LAWS and AI from a legal standpoint, which creates a number of problems, given the fact that artificial intelligence has the capability to make decisions that affect human lives.

One of the pressing emergent questions involves a machine's ability to determine who lives or dies. When we give a machine the power to make life-altering decisions, we are essentially putting our lives in the hands of technology. An example that Scherer and Jenkins use is autonomous vehicles. These vehicles drive themselves and do not require human operation, at least on a freeway or highway. When the vehicle moves onto a smaller road, however, the control of the vehicle is given back to the human. What if we were to create self-driving technology that eliminated any sort of human operation, no matter the road? In that case, we face the risk that the technology could malfunction and

14. Matthew Gault, "Ethical Behavior on the Battlefield," Interview with Pauline Kaurin, *Angry Planet: War College*, podcast MP3 audio, edited by Bethel Habte, February 28, 2017, https://podcasts.google.com/?feed=aHR0cHM6Ly9yc3MuYWNhc3QuY29tL3dhcmNvbGxlZ2U&episode=OGVmNWIxODAtODE1My00N2M4LTlmYWUtZGU2OWI3MjU5ZTcx&hl=en&ep=6&at=1569977817071.

15. Anthony C. Pfaff, "Respect for Persons and the Ethics of Autonomous Weapons and Decision Support Systems," *Real Clear Defense*, March 4, 2019, https://www.realcleardefense.com/articles/2019/03/04/respect_for_persons_and_the_ethics_of_autonomous_weapons_and_decision_support_systems_114233.html.

16. Pfaff, "Respect for Persons."

17. Ariel Conn, "Law and Ethics of Artificial Intelligence with Ryan Jenkins and Matt Scherer," *Future of Life Institute*, podcast MP3 audio, March 31, 2017, https://futureoflife.org/2017/03/31/podcast-law-ethics-artificial-intelligence/.

put not only the human passenger of the car in harm's way, but other drivers on the road as well, which then imposes an ethical crisis.[18] The same goes for autonomous weapon systems. When a human gives the power to a machine to make decisions, such as whom to target in combat or what operations to perform in wartime, the person gives up their control over the outcome of any situation brought on by the actions of the machine. If we allow machines to make lethal decisions, the individual gives up the right to any sort of human judgment.

A big debate that is currently taking place is where to draw the line between what is considered to be an autonomous weapon and what is not, as well as who is held accountable in the event that the technology malfunctions. The ICRC definition of an autonomous weapon is as follows: "Any weapon system with autonomy in its critical functions—that is, a weapon system that can select (search for, detect, identify, track or select) and attack (use force against, neutralize, damage or destroy) targets without human intervention."[19] By this definition, it can be assumed that this means any weapon not manned in any way by a human. However, there are weapons that require minimal human intervention but could still be considered autonomous or partially autonomous. These types of weapons blur the lines a bit. If there is a weapon that can function completely on its own, needing human assistance only to turn it on, who becomes accountable if the machine malfunctions or fails to do its job properly? These questions create uncertainty and confusion from a legal perspective.

The Tallinn Manual on The International Law Applicable to Cyber Warfare, edited by Michael N. Schmitt, sheds light on the gray areas in cyber warfare. A section in the manual discusses the distinction between the computer systems and the cyber infrastructure: "The cyber infrastructure is not a means of warfare because an object must be in the control of an attacking party to comprise a means of warfare."[20] Accountability rests on who is in control of the technology. The machine itself, while

18. Conn, "Law and Ethics."

19. Neil Davison, "A Legal Perspective: Autonomous Weapon Systems Under International Humanitarian Law," *International Committee of the Red Cross*, January 31, 2018, https://www.icrc.org/en/document/autonomous-weapon-systems-under-international-humanitarian-law.

20. Michael N. Schmitt, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 119, http://csef.ru/media/articles/3990/3990.pdf.

possessing lethal attack capabilities, is not at fault. Situations gain complexity when multiple people are controlling different aspects of the technology.

An ethical question that arises in these circumstances is that with the development of this new technology, will the readiness and accessibility of these machines make war more appealing to leaders? War is viewed in a highly negative context; however, if these weapons and machines can make the jobs easier for the military, it is possible that avoiding war will become less of a priority. Because of the vast difference of opinions on this matter, it is difficult to construct substantial laws surrounding LAWS and AI.

Also, artificial intelligence and lethal autonomous weapon systems are still very unpredictable, and many believe that banning the use of such technology in combat before discovering all the possibilities it holds would be premature.[21] This brings about a counterargument to the assumption that all development of AI and lethal autonomous weapons is bad. An example given in the Future of Life podcast is that if sometime later down the road humans were able to create AI that was able to distinguish between civilians and combatants and even find a way to tell who were direct participants in hostilities, that could potentially create a safer environment for the warfighter and possibly reduce the number of innocent casualties on the battlefield. In such a circumstance, the role of ethics could be flipped, and instead of this technology being feared and banned, there would be pressure to use this technology rather than continuing to put innocent lives at a high risk by putting troops on the ground.[22] These advances in technology and weapon systems have the potential to make war safer for the civilian and less brutal for the combatant, but at the same time, if it were in the hands of the wrong party, it could have the exact opposite effect. It is so crucial that as these developments continue to take place, law and policy makers must constantly search for new ways to implement laws and regulations to maintain ethics and humanity in times of war.

As the race for AI dominance escalates, it is more important than ever to put in place regulations on technological weapon developments

21. Hayley Evans, "Too Early for a Ban: The U.S. and U.K. Positions on Lethal Autonomous Weapons Systems," *The Lawfare Institute*, April 13, 2018, https://www.lawfareblog.com/too-early-ban-us-and-uk-positions-lethal-autonomous-weapons-systems.

22. Conn, "Law and Ethics."

in order to keep the public safe. China is working around the clock to achieve cyber superiority equal to or surpassing that of the United States. China claims that it "advocates for the peaceful use of cyberspace";[23] however, its economic initiatives suggest other sinister motives. With China in the race to become a technological global superpower, the United States faces a large national security threat. When dealing with the question of what regulations against AI and LAWS need to be put in place, we face yet another roadblock. The United States is fair and ethical in its dealings and strives to be a beacon of justice and law for the world. Unfortunately, many enemies of the United States do not uphold this same standard of honor. China and Russia, for example, have been notorious for playing dirty. As far as military supremacy, when it comes to artificial intelligence, the Chinese are not so far behind. In fact, they are quickly gaining on the United States. According to Bill Gertz, it is said that we are still uncertain as to how advanced the Chinese are in their developments of AI weapons and technologies.[24]

With the Chinese quickly excelling in cyber technology, international laws should be implemented to regulate the use of AI technology and lethal autonomous weapons in warfare, in the event that the Chinese or other near-peer competitors of the United State show use of force. The Commentary of New Weapons of Additional Protocol I of the Geneva Conventions states that "the use of long distance, remote control weapons, or weapons connected to sensors positioned in the field, leads to the automation of the battlefield in which the soldier plays an increasingly less important role."[25]

Use of autonomous weapons on the battlefield limits the roles of soldiers and imposes significant ethical concerns. Additionally, the commentary goes on to warn, "All predictions agree that if man does not master technology, but allows it to master him, he will be destroyed by

23. Li Zhang, "A Chinese Perspective on Cyber War," *International Review of the Red Cross* 94, no. 886 (2012): 803, https://international-review.icrc.org/articles/chinese-perspective-cyber-war.

24. Bill Gertz, "China in Race to Overtake U.S. Military in AI Warfare," *The National Interest*, May 30, 2018, https://nationalinterest.org/blog/the-buzz/china-race-overtake-us-military-ai-warfare-26035.

25. International Committee of the Red Cross (ICRC), "Commentary of New Weapons," *Treaties, States Parties and Commentaries*, 1987, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=F095453E41336B76C12563CD00432AA1.

technology."[26] The commentary supports the claim that unless new laws are written to keep AI and LAWS development in check, autonomous weapon technology, in the wrong hands, could lead to aggression and use of force.

The next question addresses what types of laws should be put in place to regulate these new technological advancements. Since the world of AI and autonomous systems is still a new concept, there is much debate as to where to set boundaries. There is no right or wrong answer as of now, but as the development of such technology continues, laws will need to adjust to maintain the security of not only participating nations, but the world. A question to be carefully considered is: what are the guidelines to follow when programming a new autonomous weapon? China does not seem to have any sort of boundaries when it comes to creating new lethal technology. Where do we draw the line at how deadly to make these weapons? It is against the law of armed conflict to inflict unnecessary suffering. Regarding artificial intelligence, what would constitute unnecessary suffering? Another vital consideration is that as AI technology matures, the laws surrounding it would have to be subject to flexibility and change. As technological advancements rapidly increase, it is important to be wary of all the possible effects that AI and LAWS could have on not only combatants during wartime but also the civilian population as well.

The future of warfare with the use of artificial intelligence and lethal autonomous weapons systems will look very different from war today, as we move away from traditional tactics and methods to incorporate new technology. As Mary L. Cummings observes, AI will only be as advanced and capable as it is programmed to be. This means that until artificial intelligence is engineered to think and reason on its own without the operation of humans, it will not be completely autonomous.[27] It is hard to say where exactly the world will be ten years from now on the cyber front; however, it is safe to say that huge steps will have been taken and many achievements made on all sides regarding technology. Hopefully, by that time there will be fewer gray areas in the legal aspects of AI and LAWS, and we will have better control over the

26. ICRC, "Commentary of New Weapons."

27. Mary L. Cummings, "Artificial Intelligence and the Future of Warfare," *Chatham House*, January 26, 2017, https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf.

direction in which this technological race is headed.

In order for the United States to stay ahead of China and other competing nations, our main focus must remain on autonomous warfare and security. As new advancements are made in the technology field, laws will need to account for the use of AI and LAWS in warfare, as it is inevitable that this technology will be ever increasing. The world is moving at a fast pace toward mastering autonomous technology. The United States no longer has a cushion of space in between itself and other technology-hungry nations. China and Russia are rapidly closing the gap in technological advancements. As we continue to maneuver the uncertainties of new and unpredictable cyber/autonomous weapons, it is imperative for policy and lawmakers to come up with clear legislation to regulate our use of this weapons technology. Whichever nation gains control over this technology first will have the upper hand in any warfare scenario. In order to stay ahead, we must constantly progress toward excelling in the industry of artificial intelligence.

Lethal Autonomous Weapons and How They Relate to International Humanitarian Law

Arik Bryton Nelson

Throughout history, warfare has paved the way for incredible technological innovation. More often than not, victory has favored those who have exploited the newest advances in technology. Robotics and automation are at the forefront of modern-day industry, and militaries everywhere spend billions of dollars to acquire the latest and greatest technology in order to gain the upper hand in combat. By removing the human element from the battlefield, the new technologies have made war safer and more efficient. As advantageous as new weaponry may be, both semiautonomous and fully autonomous weapons are not without their flaws. They raise moral, ethical, and legal questions that have yet to be answered by the international community.[1] This paper will address the legal concerns raised by the implementation of Lethal Autonomous Weaponry (LAW) in warfare and will explore the possibilities of regulating said technologies on the international level. I will begin by giving a brief definition of LAWs and their current use in warfare around the world. I will then proceed to examine the complications that LAWs pose within the framework of International Humanitarian Law (IHL)[2] before exploring the possibilities for their future regulation.

I. Introduction

A. Definitions

When one hears the term "Lethal Autonomous Weaponry," the

1. More specifically, no international treaties or agreements have been made to regulate or ban the use of autonomous weapons in warfare.

2. Also known as the law of armed conflict or simply the law of war. For consistency and simplicity, I will be referring to this as IHL. IHL is not found in any single source, but rather is a set of laws derived from various international agreements such as the Geneva and Hague conventions.

image of Skynet's killer robotic soldiers from the movie *The Terminator*, or perhaps the similarly violent robots from the movie *I, Robot* might come to mind. While the robots from these films might fit within the definition of autonomous weaponry, they certainly do not define the criteria that a piece of technology must meet in order to be considered fully autonomous. In reality, autonomous weapons, by definition, can be much simpler than a walking, human-like robot with free will. As it currently stands, automated technologies can be split into one of two categories: semiautonomous and autonomous. To understand the difference between these two definitions, one must understand the concept of the decision-making process known as the OODA (Observe, Orient, Decide, Act) loop. Created by Air Force Colonel John Boyd, the OODA loop is a decision-making process that cycles through four steps.[3] This process is often taught in the military to encourage quick decision-making during stressful situations. The main difference between a semiautonomous weapon and a fully autonomous weapon is the location of the human in the OODA loop.

In a semiautonomous weapon system, a human is located somewhere within the loop. In other words, the weapon cannot complete all four processes of the OODA loop without human approval in at least one of the steps. A good example of this can be seen with Raytheon's Upgraded Early Warning Radar (UEWR) system.[4] According to Raytheon, UEWR technology "provides early detection and precise tracking of incoming ballistic missiles as well as quick, accurate determination of threat versus non-threat objects."[5] In a video that explains the technology, Raytheon describes the technology as having the capacity to automatically detect missiles using a radar system, which alerts military personnel of an impending missile attack while it is still relatively far away. Although this system is able to detect incoming ballistic missiles without human assistance, it will not deploy any countermeasures without human approval, thus allowing the human to make the ultimate call on whether or not to use deadly force. The system effectively puts the human inside the OODA loop and makes it a semiautonomous weapon system.

3. David S. Fadok, "John Boyd and John Warden: Air Power's Quest for Strategic Paralysis," (thesis, School of Advanced Airpower Studies, 1994), 16.

4. Raytheon is a popular defense contractor for the United States and its allies.

5. "Upgraded Early Warning Radar (UEWR)," *Raytheon*, accessed December 10, 2019, https://www.raytheon.com/capabilities/products/uewr.

An autonomous weapon system, on the other hand, completely removes the human element from the decision-making process. In other words, an autonomous weapon system can find, hunt, and execute its own targets without human approval. The United States Department of Defense (DOD) directive 3000.09 describes them as such:

> A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.[6]

Currently, no countries use a fully autonomous weapon system. The technology for a LAW is still under development, and countries such as the United States, the United Kingdom, China, and Russia are close to achieving it.

B. Current Use and Legal Framework

As stated above, no country currently uses fully autonomous weapon systems. That being said, semiautonomous weapons are widely used in both defensive and offensive capacities by a variety of actors. From complex missile defense systems and Remotely Piloted Aircraft (RPA)[7] used by the United States and its allies to simple quadcopter drones used by Yemeni Houthi rebels, semiautonomous weapons are becoming quite common on the battlefield. RPAs in particular are becoming somewhat of a staple for precision airstrikes. Their popularity can be attributed to the ever-decreasing cost to deploy them, their ability to conduct extensive reconnaissance before an attack, and their being controlled from across the world.

Perhaps one of the most popular semiautonomous weapons being deployed today is the Iron Dome missile defense system that is used by Israel to defend its cities against rockets and other explosives launched by Hamas and Hezbollah. Developed by Rafael Advanced Defense Systems. Israel has used this weapon system extensively to protect its cities from short- and medium-range threats. According to Raytheon, who has partnered with Rafael with Iron Dome technology, it "detects and intercepts a variety of shorter-range targets such as rockets, artillery,

6. United States Department of Defense Directive 3000.09, (2012), 13.
7. Also known as Unmanned Aerial Vehicles (UAV) or simply drones.

and mortars."[8] While the exact numbers can only be estimated, Iron Dome technology has been able to save dozens, if not hundreds of Israeli civilians from rocket attacks.

Even though countries like the United States have their own policy that dictates the way that autonomous weapons should be used, there is currently no international legal framework that provides guidelines for the way that semiautonomous weapons and autonomous weapons should be used, whether it would impose regulations or a ban altogether. Semiautonomous weapons are not inherently problematic, and current international laws are enough to govern their use on the battlefield.

Autonomous weapons, however, raise a number of legal questions. If a human is not in the decision-making process, what assurance is there that the LAW being used will be able to follow strict laws and rules of engagement that often require human judgment? Furthermore, can a LAW ever appropriately adhere to the principles of distinction and proportionality in warfare? I will now discuss the legal concerns raised by LAWs and how they relate to the IHL principles of humanity, distinction, and proportionality.

II. Legal Complications

A. Humanity

Humanity is an all-encompassing principle that is intended to prevent the unnecessary suffering of both civilians and combatants in any given conflict. Perhaps the best definition of humanity in warfare is outlined in article 22 of the Hague conventions of 1899 and 1907, which states that "the right of belligerents to adopt means of injuring the enemy is not unlimited."[9] The following article of the same convention outlines more specific prohibitions, such as, "to kill or wound an enemy who . . . has surrendered at discretion" or, "to declare that no quarter will be given."[10]

Accepting surrender is a fundamental part of the principle of humanity. This is one of the biggest weaknesses and problems that LAWs

8. "Iron Dome and SkyHunter Systems," *Raytheon*, accessed December 13, 2019, https://www.raytheon.com/capabilities/products/irondome.

9. *The Hague*, Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 18 October 1907, article 22.

10. *The Hague*, 1907, 23 (C, D).

will face. Throughout history, soldiers who surrender to their enemies have typically displayed some sort of symbol or gesture to display their submission, such as waving of a white flag or simply throwing down their weapons and raising their hands above their heads. A belligerent to a conflict is not required by IHL to give their enemy a chance to surrender before killing them, but they are obligated to accept the surrender if one is given. When this principle is applied to LAWs, the question arises as to whether a LAW would be able to recognize a surrender in any capacity. Furthermore, would a LAW be able to take prisoners appropriately and escort them to a designated location after the time of their surrender? While the software designed to govern the exact decisions of any given LAW is still in development, recognizing and accepting surrender has always required a human decision, and even humans occasionally make the wrong decision. Additionally, if a LAW were ever able to accept surrender, what would stop an adversary from simply feigning surrender to deceive the LAW and gain the upper hand? Other complicated principles of humanity present problems to LAWs, such as not causing superfluous injury or unnecessary suffering, as is outlined in another section of article 23 of the Hague Conventions.[11] While LAWs can be outfitted with specific weapons that are compliant with this regulation, they would also need to be programmed not to deliberately cause unnecessary injuries to their targets.

B. Distinction and Discrimination

The principles of distinction and discrimination exist to protect the civilian population during wartime. Distinction is the concept that any given military must be able to distinguish between military and civilian targets, whether they be objects or people, in any given attack that they conduct. Likewise, the principle of discrimination dictates that if a weapon is to be used, it must be able to strictly target military personnel or objects. A good example of an indiscriminate weapon is poison gas. Used extensively in World War I, poison gasses were mostly used to flush enemy troops out of trenches. While the effectiveness of gas on the battlefield has always been questioned, the potential harm that it can cause to the civilian population is certain. Indeed, if the wind changes direction on a day that poison gas is launched, it could blow the toxic fumes into a nearby town full of innocent civilians. This inability of poison gasses to discriminate ultimately led to them being

11. *The Hague*, 1907, 23.

banned on an international level by the Geneva Protocol of 1925.[12]

While LAWs can be equipped with specific weapons that are discriminate, the ability of a LAW to distinguish a military target from a civilian target before applying lethal force is questionable. If warfare were as simple as it were in centuries past, perhaps distinction would not be an issue for LAWs. One would simply need to program the system to target anything bearing an enemy flag or uniform. Unfortunately, the fact of the matter is that today's wars are often fought in the midst of civilian populations, where fighters either wear no distinguishing uniforms or deliberately try to blend in with the civilian population to deceive their adversaries. Even human soldiers frequently struggle with this principle. Indeed, the wars in Afghanistan and Iraq have proven themselves to be nightmares when it comes to distinction. Paul Scharre, an expert on the subject of LAWs, described the problem of distinction in his book *Army of None* as follows:

> Distinguishing people would be far and away the most difficult task. Two hundred years ago, soldiers wore brightly colored uniforms and plumed helmets to battle, but that era of warfare is gone. Modern warfare often involves guerrillas and irregulars wearing a hodgepodge of uniforms and civilian clothes. Identifying them as a combatant often depends on their behavior on the battlefield. I frequently encountered armed men in the mountains of Afghanistan who were not Taliban fighters. They were farmers or woodcutters who carried firearms to protect themselves or their property. Determining whether they were friendly or not depended on how they acted, and even then was often fraught with ambiguity.[13]

Being able to spot the differences between civilians and enemy combatants is a crucial part of adhering to IHL and would be a difficult task for a LAW. In addition to the difficulties of distinguishing civilians from military targets, LAWs could face the problem of fratricide,[14] as enemy fighters could be confused for allies, especially if they were from a different faction than the LAW, such as Iraqi or Afghan security forces.

12. *Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare*, Geneva, 1925.

13. Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton, 2018), 253.

14. Fratricide is the killing of one's comrades or allies.

Although the technology is still in development, it must be acknowledged that distinction would be perhaps the most difficult IHL principle for a LAW to follow.

C. Proportionality

Sometimes referred to as "collateral damage," the principle of proportionality dictates that parties to a conflict must "refrain from attacks in which the expected civilian casualties will be excessive in relation to the anticipated military advantage gained."[15] While the acceptable amount of civilian collateral damage in an attack varies from country to country, most states agree that the acceptable amount of damage cannot be simply calculated with numbers. In the *DOD Law of War Manual*, the United States elaborates on this concept by stating:

> Determining whether the expected incidental harm is excessive does not necessarily lend itself to quantitative analysis because the comparison is often between unlike quantitates and values. The evaluation of expected incidental harm in relation to expected military advantage intrinsically involves both professional military judgments as well as moral and ethical judgments evaluating the risks to human life.[16]

Soldiers must often make judgment calls on whether something is proportional in the heat of battle, and they do not always have the means to call up a JAG to ask if what they are about to do is okay.[17] As is stated above, moral and ethical judgments are required when making decisions involving damage evaluation, which is something that a LAW would inherently lack. This could be easily solved by ensuring that a human is present to determine whether the proportionality is appropriate, but by removing the decision-making element from the LAW and inserting the human back into the OODA loop, the LAW effectively reverts from being fully autonomous to simply being a semiautonomous weapon system.

While not impossible, it would be difficult for LAWs to be able to

15. Laurie R. Blank and Gregory P. Noone, *International Law and Armed Conflict: Fundamental Principles and Contemporary Challenges in the Law of War* (New York: Wolters Kluwer, 2019), 51.

16. *United States Department of Defense Law of War Manual*, Office of the General Counsel, 2015, 256.

17. Judge Advocate General, also known as a military lawyer. JAGs advise commanders on the legalities of attacks and operations.

follow all of the specific principles outlined in IHL, but with the current lack of regulations on LAWs, the possibility that they will break IHL principles is higher. I will now discuss the possibilities of regulating LAWs by providing a brief history of weapons regulation and examining where they could possibly fit within the existing international legal framework.

III. Regulating LAWs

A. A Brief History

Beginning in the late 1800s, a multitude of international agreements have been made in an effort to minimize the suffering caused by war. Some agreements, such as the Hague and Geneva conventions, have developed principles such as those discussed earlier that are designed to encompass all weaponry. In more recent years, treaties have been signed that regulate or ban the use of specific technologies in warfare, such as the Chemical Weapons Convention and the Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons. More often than not, as unfortunate as it is, many of these agreements were not made until after both civilians and combatants suffered due to IHL violations. It is possible, however, to regulate or prohibit the use of a specific weapon before it becomes a problem. Indeed, the St. Petersburg Agreement, one of the first contemporary treaties dealing with IHL, and the first to prohibit the use of a specific weapon in warfare, was created to ban the use of small explosive projectiles, specifically those weighing less than 400 grams, before they could ever be used in warfare.

This particular treaty laid the groundwork for future agreements. The closing statement of the declaration states,

> The Contracting or Acceding Parties reserve to themselves to come hereafter to an understanding whenever a precise proposition shall be drawn up in view of future improvements which science may effect in the armament of troops, in order to maintain the principles which they have established, and to conciliate the necessities of war with the laws of humanity.[18]

18. "Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight," Saint Petersburg, 29 November/11 December 1868, http://hrlibrary.umn.edu/instree/1868b.htm.

This treaty was not only effective in its purpose of banning exploding bullets, but also for establishing a tradition of evaluating new advances in technology and determining whether they can comply with the laws of humanity. The advancement in automation technology is accelerating more and more every day, and while no current international agreement prohibits or regulates the use of LAWs, it is not impossible to establish a regulation within the legal framework that already exists, namely the Convention on Certain Conventional Weapons (CCW).

B. LAWs in the CCW

The CCW currently regulates a number of weapons such as land mines, booby traps, and even blinding laser weapons.[19] When the CCW was first drafted in 1980, however, it contained regulations only for non-detectable explosive fragments, land mines, and incendiary weapons. The CCW was designed to be open ended in order to allow future weapons to be regulated. In fact, the additional regulations on lasers and explosive remnants were not added until 1995 and 2003, respectively. The protocol on land mines was amended in 1996. Parties to the convention meet on an annual basis to review the agreement and discuss the possibilities of new protocols and amendments. The ICRC describes it as such:

> States Parties meet annually to review the status and operation of the CCW and its Protocols. Regular meetings of governmental experts are held to facilitate the implementation of these instruments and to consider new issues that may be appropriate for regulation under the CCW, such as anti-vehicle mines, cluster munitions and lethal autonomous weapons systems.[20]

In article 8 (2) of the convention itself, the exact method for adding a new protocol is laid out:

> At any time after the entry into force of this Convention

19. International Committee of the Red Cross (ICRC), "Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects," Geneva, 10 October 1980, https://www.icrc.org/en/doc/assets/files/other/icrc_002_0811.pdf.

20. ICRC, "Advisory Service on International Humanitarian Law, 1980 Convention on Certain Conventional Weapons—Factsheet," accessed August 2018, https://www.icrc.org/en/document/1980-convention-certain-conventional-weapons.

> any High Contracting Party may propose additional protocols relating to other categories of conventional weapons not covered by the existing annexed Protocols. . . . Such a conference may agree, with the full participation of all States represented at the conference, upon additional protocols which shall be adopted in the same manner as this Convention, shall be annexed thereto and shall enter into force as provided in paragraphs 3 and 4 of Article 5 of this Convention.[21]

International agreements are never an easy task. Adding an extra protocol into the CCW to regulate the use of LAWs would certainly come with complications and pushback from one or more parties, but it is arguably the best, currently existing piece of international law that can prohibit or ban their use.

IV. Conclusion

LAWs can certainly provide a combat advantage to whoever uses them. Even semiautonomous weapons have proven to be effective in minimizing casualties and stopping enemy attacks. Although they are still in development, LAWs already face a lot of complications when it comes to compliance with the principles of IHL, especially with regards to humanity and distinction. If they ever reach the battlefield, LAWs will present challenges to such principles. It can be argued that no matter how well the programming on a LAW may be, it can never replace the necessary element of human judgment in combat, therefore making adherence to IHL nearly impossible. Although individual countries may have policies that govern the use of LAWs, no international agreements that regulate their use in warfare currently exist. Because of the open nature of the CCW, it is perhaps the most effective way to establish regulations on LAWs before they become an international problem.

21. ICRC, "Convention on Prohibitions."

Mexican Drug Trafficking Organizations, ISIS, and Other FTOs

Joshua Jones

The Sinaloa drug cartel's skirmish with the Mexican federal government raises questions about the power of Mexican Drug Trafficking Organizations, hereafter referred to as MDTOs, if they become involved in exploiting the southern border with members of ISIS and other terrorist organizations[1] that seek to illegally enter the US.[2] This paper argues that in the hypothetical scenario of MDTOs aiding ISIS or any other Foreign Terrorist Organization, hereafter FTO, in getting to the US for purposes of terrorism indefinitely, the MDTOs should be considered parties to the conflict between the US and ISIS. This paper assumes that the legal argument for the US war on ISIS is permissible.[3]

MDTOs have similar command and control structures to many FTOs, with arms and monetary means to accomplish their objectives. However, members of MDTOs are often members of the civilian population. Article 51(3) of Additional Protocol I states, "Civilians shall enjoy the protection afforded by this section, unless and for such times as they take a direct part in hostilities."[4] In order to keep these protections, civilians have a strict obligation to not engage in warfare during an armed conflict. Otherwise, civilians involved with MDTOs would forfeit the protections given to them of being non-targetable by the

1. U.S. Congress, House of Representatives, Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, *Threat to the Homeland: Iran's Extending Influence in the Western Hemisphere*, 113th Congr., 1st sess., July 9, 2013.

2. Ardian Shajkovci Speckhard, "PERSPECTIVE: ISIS Fighter Claims Attack Plot Via Mexico, Underscoring Border Vulnerability." *Homeland Security Today*, 2019.

3. There is much debate among law of war scholars about the legality of the war on ISIS by the US and whether existing US law provides sufficient legal groundwork for the war. See source on footnote 16 for discussion.

4. API, art 51, 1977.

military.[5] MDTOs are already engaged in illegal activity, including human trafficking and drug smuggling, and will, in many cases, smuggle anyone into the US for the right price. If an MDTO did this continuously, knowingly or unknowingly, for members of ISIS or other FTOs, this would be seen as a violation of the law of war, which defines what conduct is allowed between warring nations. This aid from an MDTO could be induced by the MDTO's and an FTO's mutual ties to the international drug trade and could include fabricating passports or visas for FTOs or smuggling FTO members through known human trafficking routes.

Treatment of law of war violations has a precedent in US law. In the landmark Supreme Court decision *Ex Parte Quirin*,[6] The Supreme Court ruled against eight German saboteurs who were trained in Germany to land in the US carrying explosives, intending to attack areas of commercial importance during WWII. The court concluded that these eight men were spies without uniform, enemy belligerents within the meaning of the Hague convention,[7] whose purpose was sabotage. It was determined these men had violated the law of war, and they were classified as unlawful enemy combatants.

Ex Parte Quirin was a landmark decision because it was the first time the highest US court ruled on a law of war issue and it introduced the term "unlawful enemy combatant" into the US common law. Under the Military Commissions Act of 2006, congress codified the term "unlawful enemy combatant" into statutory law with the definition that it is (i) a person who has engaged in hostilities or who has purposefully and materially supported hostilities against the United States or its co-belligerents who is not a lawful enemy combatant (including a person who is part of the Taliban, al Qaeda, or associated forces); or (ii) a person who, before, on, or after the date of the enactment of the Military Commissions Act of 2006, has been determined to be an unlawful enemy combatant by a Combatant Status Review Tribunal or another competent tribunal established under the authority of the President or the Secretary of Defense."[8]

5. "Conflicts Not of an International Character," *IHL Databases ICRC*, accessed February 2, 2020, https://ihl-databases.icrc.org/ihl/WebART/375-590006.

6. *Ex Parte Quirin*, 317 US 1 (1942).

7. *Ex Parte Quirin*, 317 US 1 (1942).

8. United States Congress, "Military Commissions Act of 2006," 3, https://www.govinfo.gov/content/pkg/BILLS-109s3930es/pdf/BILLS-109s3930es.pdf.

Ex Parte Quirin was also significant because it established that enemy spies could be prosecuted by military courts and would not be allowed to have a trial-by-jury.[9] Essentially, the case established precedent for how enemy agents would be prosecuted by the US government during war time.

In another Supreme Court case, *Johnson v. Eisentrager*, non-resident enemy aliens were tried and convicted by a military tribunal for violations of the law of war committed in China prior to their capture. The captured immigrants were transported by the American military to the American-occupied part of Germany and were imprisoned there by the military. The immigrants petitioned the District Court of the District of Columbia for writ of habeas corpus, directed to the Secretary of Defense and the army officers with power over the immigrants' custody. However, the District Court held that nonresident aliens with whom the US is at war have no access to US courts during wartime. The court also held that the US Constitution does not bestow a right of protection or immunity from war trial and punishment on an alien enemy engaged in adverse service of a government that is at war against the US.[10]

These cases establish precedent that Constitutional protections do not apply to enemy alien residents outside the jurisdiction of the US.[11] This is significant, because were MDTOs to aid ISIS or any other FTO in entering the US, a Combatant Status Review Tribunal could deem these MDTOs as unlawful enemy combatants. If FTO-aiding MDTOs were considered unlawful enemy combatants, they would violate the law of war, be considered parties to the conflict between the US and ISIS, lose their protected civilian status, and render themselves prosecutable under military tribunals, with no access to the US court system.[12] Additionally, under Article 4 of the Geneva Conventions of 1949, Mexican Drug Trafficking Organizations would not be able to qualify for prisoner of war status, because they are engaging in unlawful acts

9. "*Ex Parte Quirin*—Significance," *Significance—War, Court, Military, and Courts—JRank Articles*, accessed October 29, 2019, https://law.jrank.org/pages/25474/Ex-Parte-Quirin-Signifincance.html.

10. *Johnson v. Eisentrager*, 339 US 763 (1950).

11. Johnson v. Eisentrager.

12. "Protection of the Civilian Population," *IHL Databases ICRC,* accessed November 15, 2019, https://ihl-databases.icrc.org/ihl/WebART/470-75006.

against the US and are not lawful combatants.[13] This article leads to the same conclusion that MDTOs committing illegal acts under the law of war would lose their civilian status and would only be able to claim Common Article 3 protections set forth under the Geneva Conventions, which defines humane treatment of detained persons.[14] This situation is most likely to occur outside the jurisdiction of the US.

In further support of this conclusion about the status of hypothetical FTO-aiding MDTOs, the Law of War Manual for the Department of Defense clarifies that

> unlawful combatants or 'unprivileged belligerents' are persons who, by engaging in hostilities, have incurred one or more of the corresponding liabilities of combatant status (e.g., being made the object of attack and subject to detention), but who are not entitled to any of the distinct privileges of combatant status.[15]

This definition is important in understanding that the US government will not recognize combatant status by civilians, and civilians involved with FTO-assisting MDTOs would not receive any privileges that legal combatants otherwise receive under prisoner of war status. These hypothetical MDTOs would not be able to claim this status because they are not legal combatants, they are civilians participating illegally in warfare. Such MDTOs would be classified as Non-State Armed Groups, hereafter referred to as NSAGs. Again, this leads to the conclusion that such NSAG-classified MDTOs would be considered parties to the conflict, direct participants in FTO hostilities, and, in part, responsible for the actions committed by these terrorist groups.

Thus, the US can argue legal justification for self-defense against MDTOs that continuously assist ISIS or any other FTOS in entering the US, because these MDTOs would become parties to the conflict. This follows the same logic as the US's current justification of the war with ISIS. The US government has legally justified its war with ISIS

13. "Prisoners of War," *IHL Databases ICRC*, accessed November 23, 2019, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=2F681B08868538C2C12563CD0051AA8D.

14. "Conflicts Not of an International Character."

15. Department of Defense, *DoD Law of War Manual*, Washington, DC: Department of Defense, accessed December 2, 2019, https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-1.

pursuant to its legal interpretation of the Authorization for Use of Military Force, which gives the US legal ground to conduct its war against Al-Qaeda and associated forces. The US Government argues that because ISIS is a split-off group from Al-Qaeda, the US has legal ground to use the military to conduct attacks against them.[16] By the same principle, MDTOs who become parties to the conflict could be subject to attack by the US military.[17] Again, this implies the US military would be able to conduct military operations against ISIS or FTO-aiding MDTOs, prosecute them via military tribunals, and conduct airstrikes against them in concordance with the law of proportionality and the Geneva Conventions.[18]

This conclusion operates under the assumption that such MDTOs hypothetically provide aid to ISIS willingly. The principle of effective control, which determines responsibility of a state to an armed group in order to conduct war against another state, applies to armed groups when determining the collective responsibilities of individuals' actions. In *Tadic v. Prosecutor*, the principle of "overall control" was established, and it created criteria concerning how much control a state has over armed forces when using them to conduct military attacks against another state.[19] ISIS is here considered a state. With regards to MDTOs aiding members of ISIS, it would be important to distinguish whether the MDTOs were coerced into aiding them in entering the US, or if it was a mutually assured transaction. If the MDTOs were coerced into aiding ISIS or other FTOs into the US, these terrorist groups would bear the sole responsibility. Other cases also indicate state responsibility for actions committed by organized armed groups, and the same principle would apply to ISIS were it to ally itself with a MDTO.

The International Court of Justice, hereafter ICJ, set out legal conclusions regarding state responsibility for the actions of the individual in *Nicaragua v. US*. This case created the effective control test previously mentioned. In this case, the ICJ ruled that because the US armed the

16. Patricia Stottlemyer, "Is the War Against ISIS Legal?" *Just Security*, February 23, 2018, https://www.justsecurity.org/52896/doe-v-mattis-war-isis-legal/.

17. "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)," 1977, *IHL Databases ICRC,* https://ihl-databases.icrc.org/ihl/INTRO/470.

18. "Conflicts Not of an International Character."

19. *Prosecutor v. Tadic*, IT-94-AR72, Appeals Chamber, Decision, 2 October 1995.

contras against the government of Nicaragua and exercised effective control over them, the US government was legally responsible for the actions of the contras.[20] These armed groups were parties to the conflict due to their rebellious actions against Nicaragua. This case establishes the previous conclusion concerning the state's responsibility when using military organized groups.

In the event of a US military attack occurring, the State of Mexico would object to military intervention within their jurisdiction. However, the US would not need consent from Mexico because of its war on ISIS and other FTOs, and those who become parties to the conflict. There is precedent for the US not needing consent from states to conduct attacks against highly organized terrorist groups in another state's territory, such as the Osama Bin Laden raid in Pakistan and the more recent Al-Baghdadi raid in Syria.

Recently, in Culiacan, Mexico, the Mexican military was outgunned by Sinaloa drug cartel members in a series of violent clashes that resulted in 14 police members being killed and the Mexican military conceding to release the son of MDTO leader Joaquin "El Chapo" Guzman from custody.[21] US Senator Ben Sasse (R-NE) stated that the situation demonstrated that Mexico is "dangerously close" to becoming a failed state.[22] The sentiment has been echoed by several Congress members in recent years. Mexico is in a dangerous situation because of public corruption from drug cartels. ISIS could easily take advantage of a failed state in Mexico, which shares a 2,000-mile-long border with the US.

Were this situation to occur, MDTOs would have opportunities to aid ISIS or other FTOs in entering the US. This could occur in several different ways because the groups have mutual commercial interests, including the international drug trade.[23] In order to operate, both

20. *Nicaragua v. United States of America*, Military and Paramilitary Activities, Judgement of 27 June 1986, https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-1-00-EN.pdf.

21. Ed Vulliamy, "Mystery of Mexico's Cartel Wars Grows as 'The Mouse' Is Rescued," *The Guardian*, October 20, 2019, https://www.theguardian.com/world/2019/oct/20/deadly-battle-mexican-drug-lord-cartels-el-chapo-son.

22. Ben Sasse, "Sasse Statement on Cartel Attack on Americans," 2019, https://www.sasse.senate.gov/public/index.cfm/2019/11/sasse-statement-on-cartel-attack-on-americans.

23. US Congress, House, Committee, Threat to the Homeland, "19 of the 43 US-Designated Foreign Terrorist Organizations Are Definitively Linked to the Global Drug Trade."

groups draw money from the drug trade internationally to replenish themselves financially. These similar commercial interests could be used to finance a way to hop from country to country, eventually landing in the US.

However, if Mexico became a failed state, and MDTOs engaged with FTOs in their mutual ties to the international drug trade, it would only put the US on increasingly strong legal ground in labeling MDTOs as parties to the conflict. MDTOs continuously enabling ISIS or other illegal combatants to enter the domestic US in order to commit terrorist acts would almost certainly be considered parties to the conflict. This would also apply to MDTOs actively participating in the conflict by having illegal commercial transactions with ISIS through the international drug trade. In conclusion, it would not bode well for any drug cartels that might aid ISIS or any other related terrorist groups in entering the US, as they would find themselves subject to US military action without the protection of either a civilian or lawful combatant status.

UNCLOS, America, and the South China Sea

Bryce Krieger

In July of 2016, the Arbitral Tribunal appointed under the United Nations Convention on the Law of the Sea (UNCLOS) ruled in favor of the Philippines over the South China Sea (SCS) dispute.[1] In specific, the court found that Mischief Reef was a low-tide elevation on the Philippines' continental shelf and that China's building and militarization of this region were violations of the Philippines' sovereign rights.[2] Regardless, since this ruling, China has made no effort to correct its actions and has continued to build and militarize. As such, foreign nations have called on the United States Senate to ratify UNCLOS in order to increase its credibility and to assist in settling the dispute by creating a precedent of participation among great powers.[3] This paper will demonstrate how UNCLOS has failed to settle the SCS dispute between China and the Philippines and will prove that United States' ratification of UNCLOS will not assist in mitigating the conflict. The assertions will be proven through analysis of the purpose and function of UNCLOS and the background of the SCS dispute with a specific focus on the China–Philippines dispute. Using this analysis, the paper will review the effectiveness of the UNCLOS decision to determine its failure in settling the SCS dispute, and it will discuss how the United

1. Hao Duy Phan and Lan Ngoc Nguyen, "The South China Sea Arbitration: Bindingness, Finality, and Compliance with UNCLOS Dispute Settlement Decisions," *Asian Journal of International Law* 8, no 1 (January 2018): 36, https://doi.org/10.1017/S2044251317000121.

2. Edward Friedman, Jessica Chen Weiss, M. Taylor Fravel, Orville Schell, Peter Dutton, and Tom Nagorski, "What Is the Future of the South China Sea?" *Foreign Policy*, July 12, 2016, https://perma.cc/Q7AU-SRWC.

3. Douglas W. Gates, "International Law Adrift: Forum Shopping, Forum Rejection, and the Future of Maritime Dispute Resolution," *Chicago Journal of International Law* 18, no. 1 (Summer 2017): 316–18.

States could further its participation in the dispute by ratifying UNCLOS, a move that would do little to help mitigate the SCS dispute but would be beneficial for other purposes.

United Nations Convention on the Law of the Sea

UNCLOS was created as a method to settle "all issues relating to the law of the sea" in a "spirit of mutual understanding and cooperation" as a means to maintain global "peace, justice and progress."[4] One reason for the creation of UNCLOS was the realization that disputes and problems concerning ocean space and the sea are interrelated and should be considered as a whole. The Convention was formed with the international system in mind; its goals are to "contribute to the realization of a just and equitable international economic order" by means of "the strengthening of peace, security, cooperation and friendly relations among all nations in conformity with the principles of justice and equal rights," and it "will promote the economic and social advancement of all peoples of the world."[5] Of specific importance to the SCS dispute is the Convention's reference to the United Nations General Assembly's resolution 2749, which declares that the seabed, the ocean floor, and all of its resources are "common heritage of mankind,"[6] and that the exploration or exploitation of such shall be for the benefit of all mankind. The resolution expresses a shared ownership of resources found under the sea floor, such as oil and natural gas, and it excludes the exploration of such areas for singular gain. Along with these goals and desires, the Convention sets forth rules and regulations for all aspects of the sea, including limits to territory, rights of navigation, and definitions of words and phrases such as "rocks," "islands," and "exclusive economic zones."[7]

Aligned with the general purpose of the United Nations (UN), UNCLOS' core function is to encourage peaceful resolutions and discourage the use of force. To help with the resolution process, UNCLOS established the International Tribunal for the Law of the Sea (ITLOS), but it allows each case to be sent to the court of the dispu-

4. "Oceans and Law of the Sea United Nations," *United Nations Convention on the Law of the Sea of 10 December 1982*, accessed September 29, 2019, https://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm.

5. "Oceans and Law of the Sea," *United Nations Convention*.

6. "Oceans and Law of the Sea," *United Nations Convention*.

7. "Oceans and Law of the Sea," *United Nations Convention*.

tants' choice. In addition, ITLOS can issue advisory statements on the Convention's laws and regulations so that states may establish the legality of actions before they are taken.[8] While the court of choice may change from dispute to dispute, all decisions made by tribunals receiving jurisdiction from UNCLOS are final and binding; however, they are only binding upon the parties of the particular dispute. Similar to other international courts and tribunals, UNCLOS lacks an enforcement mechanism.[9] In relation to the SCS dispute, it is important to note that while China was an original signatory to the Convention, China added qualifications to its participation in UNCLOS, including a commitment to resolve border disputes through bilateral negotiations.[10]

In recent years, UNCLOS has participated in the resolution of several maritime disputes. In a dispute between lower power states, Saint Vincent and the Grenadines submitted a case to ITLOS against Guinea for the arrest and detainment of the vessel *M/V Saiga*. In 1999, ITLOS issued its finding that Guinea had violated the rights of Saint Vincent, and as a result ITLOS ruled that Guinea must pay compensation to Saint Vincent; Guinea complied by 2001.[11]

In a separate case involving a more powerful state, Ireland initiated an arbitral proceeding against the United Kingdom (UK). While the UK originally objected ITLOS' jurisdiction, within a few weeks of the first ruling, the UK and Ireland issued reports together, indicating their cooperation with the tribunal. Within a few years, Ireland withdrew the case, satisfied with the cooperation they had received from the UK.[12] Therefore, UNCLOS has played a significant role in disputes between both low-power and high-power states, which are similar to the China–Philippines dispute.

The South China Sea

The SCS is the subject of a global dispute with the possibility for drastic consequences.[13] The controversy concerns the Paracel and Spratly

8. Gates, "International Law Adrift," 295.

9. Phan and Nguyen, "South China Sea Arbitration," 37, 44.

10. Gates, "International Law Adrift," 312–13.

11. Phan and Nguyen, "South China Sea Arbitration," 45.

12. Phan and Nguyen, "South China Sea Arbitration," 46.

13. Stephen J. Hartnett and Bryan R. Reckard, "Sovereign Tropes: A Rhetorical Critique of Contested Claims in the South China Sea," *Rhetoric & Public Affairs* 20, no. 2 (Summer 2017): 292, https://doi.org/10.14321/rhetpublaffa.20.2.0291.

islands, hundreds of other land masses, and the resources within that territory, both in the sea and under the seabed. Parts of the disputed territory are claimed by Japan, South Korea, Taiwan, Vietnam, Cambodia, Thailand, Malaysia, Singapore, Brunei, and Indonesia, while China makes a claim to the whole of the SCS. Out-of-region powers such as India and the United States also desire the right for freedom of trade and navigation in the region.

In the China–Philippines dispute alone, China has occupied, developed, and militarized Mischief Reef, territory formally annexed by the Philippines' government in the 1970s; they have since occupied eight islands.[14] China's actions are spurred by its historic claim to the entirety of the SCS through the "nine-dash line," a claim that can be traced back to the Silk Road and as early as 221 BC, when China controlled over 132 islands in the SCS.[15] With this claim, China has constructed artificial islands and built military bases on them in the middle of the SCS where no land masses had breached the surface before.[16] China's move has been challenged by several of the nations bordering the SCS, as well as the United States, which has patrolled warships through the SCS' waters in a form of protest to show that they will not recognize China's sovereignty claims.[17]

However, the SCS has much more to offer than territory. In total, close to 5.3 trillion dollars in trade passes through the SCS annually. The cargo includes about one-third of the world's oil and half of the world's liquified natural gas, and thus the conflict creates an energy security concern for the adjacent states that rely on these resources.[18] In addition, while these energy sources are traded through the region, there are more resources beneath the ocean floor. Up to 11 billion barrels of oil and 190 trillion cubic feet of natural gas deposits lie untapped underneath the SCS as well as precious metals and more common resources, such as the fish in the water. While some of the more common

14. Melissa Castan, "Adrift in the South China Sea: International Dispute Resolution and the Spratly Islands Conflict," *Asia Pacific Law Review* 6, no. 1 (1998): 97, 102, https://doi.org/10.1080/18758444.1998.11788054

15. Sean P. Belding, "China's Island Building in The South China Sea: Collateral Effect on the UNCLOS and Potential Solutions," *Houston Journal of International Law* 40, no. 3 (Summer 2018): 1009, https://link.gale.com/apps/doc/A584177014/ITOF?u=utahvalley&sid=ITOF&xid=92747b84.

16. Hartnett and Reckard, "Sovereign Tropes," 292.

17. Hartnett and Reckard, "Sovereign Tropes," 322–23.

18. Belding, "China's Island Building," 1006.

resources seem less important, the SCS provides roughly 3.7 million fishing industry jobs[19] and ten percent of the world's annual catch of fish, adding to the tension in the area.[20]

Responses to the Arbitral Tribunal's Decision

After China's invasion of Mischief Reef and militarization of the SCS, the Philippines challenged China's claim to sovereignty over the SCS by the means established through UNCLOS.[21] As a result, the Permanent Court of Arbitration in the Hague, The Netherlands, which received the Philippines' challenge, rejected China's claim. It ruled that China violated UNCLOS, that China had no historic basis to claim the SCS as sovereign territory, and that the scattering of rocks and reefs within the SCS did not qualify for exclusive economic zones.[22] However, China has claimed that denying and refusing to participate in the arbitral proceedings is a right of sovereign states, and, therefore, they are under no obligation to accept the findings of or participate in the arbitration.[23]

China's refusal to participate in the arbitration goes beyond a mere power struggle. In 2002, China formed an agreement with the Association of Southeast Asian Nations (ASEAN), in which it was determined that the SCS dispute would be settled through bilateral negotiations. China argues that the Philippines have removed the dispute from bilateral negotiations, departing from the appropriate method of settling the dispute.[24] As such, China has continued to ignore UNCLOS as a multilateral method of solving the dispute while continuing to maintain that bilateral negotiations are the appropriate setting for progress.[25]

China's refusal was not an abnormal action; similar behavior has been seen by other rebellious states, namely Russia.[26] This is part of a larger trend practiced by great powers as they ignore international organizations and deny justice to their less powerful neighbors. However,

19. Belding, "China's Island Building," 1007.

20. Stephen Wakefield Smith, "ASEAN, China, and the South China Sea: Between a Rock and a Low-Tide Elevation," *University of San Francisco Maritime Law Journal* 29, no. 1 (2016): 40.

21. Gates, "International Law Adrift," 313.

22. Friedman et al., "What Is the Future of the South China Sea?"

23. Gates, "International Law Adrift," 316.

24. Gates, "International Law Adrift," 315.

25. Castan, "Adrift in the South China Sea," 102.

26. Gates, "International Law Adrift," 290.

China's aggressive actions in the SCS and against the Philippines are particularly damaging to dispute resolution mechanisms.[27] Not only do China's actions undermine their neighbors' sovereignty, but they also undermine international governance as a whole. China's actions have infringed on several rights protected through UNCLOS and the UN. The offenses include infringements on the freedom of navigation and infringements on sovereignty through the militarization of artificial islands within their neighbors' sovereign borders. Because of the tribunal's rulings, China's actions legally constitute annexation of territory by the use of force and may be seen as acts of war.[28] Regardless, other than movements made by the United States to strengthen its military presence in the region, China has not been forced to face any substantial consequences.[29]

China has declared three main arguments against the UNCLOS decisions: first, the arbitration went forward without China's participation or consent and was therefore illegal; second, the Arbitral Tribunal did not have proper jurisdiction; third, the Arbitral Tribunal was not a legitimate source for the arbitration. However, close inspection of these complaints reveals them to be inadequate arguments. According to the UNCLOS document, China's protest of absence in the arbitration does not result in a lack of consent to the tribunal's jurisdiction, nor does it render the arbitration illegal. Likewise, while arguments relating to a tribunal's jurisdiction are not uncommon in international courts, under UNCLOS complaints are to be settled by the tribunal through proper channels. Despite this, China made its complaints known through several non-traditional channels, but never argued either orally or in writing with the tribunal itself. While the tribunal attempted to respond to China's complaint and establish jurisdiction, the tribunal's actions have likewise been ignored by China.[30] With such flimsy arguments and as an original signatory to UNCLOS, it is hard to legitimize China's choice to ignore a finding by an authorized tribunal that has been agreed upon as final and binding through the UNCLOS document.

As China continues to ignore the Arbitral Tribunal's decision, it will continue to violate the Philippines' sovereignty. This is a matter of concern for a number of other states, particularly those who are fearful of

27. Gates, "International Law Adrift," 319.
28. Belding, "China's Island Building," 1014–17.
29. Belding, "China's Island Building," 1027.
30. Phan and Nguyen, "South China Sea Arbitration," 40–42.

China's lack of respect for its smaller neighbors. While China's actions may negatively affect China's reputation as an emerging world power and portray it as belligerent and impatient regarding international law, because of UNCLOS' lack of an enforcement mechanism, any punishment is left to major powers willing to challenge China's actions.[31]

Though UNCLOS lacks any enforcement mechanism, it may affect the SCS situation. Certainly, China is capable of continuing to ignore the court's findings; however, China cannot ignore the impact the ruling will have on other states' perception of the SCS dispute. As such, perceptions of right and wrong actions within the SCS will be altered, and China's ability to act without moral implications will inevitably be affected. An optimistic view is that these new perspectives will improve bilateral negotiations in the region and narrow China's future actions.[32] Regardless, because of UNCLOS' inability to quell China's actions and restore peace and stability in the SCS, the institution has not resolved the dispute.[33]

Collateral Effects

While UNCLOS may have failed in settling the SCS dispute, its ruling will cause collateral effects in other regions of the world. As mentioned, this ruling will potentially alter China's future interactions with its neighbors and with other great sea powers such as the United States.[34] Of particular note, the decision will influence interactions between states in the Arctic, the Gulf of Mexico, and the Strait of Hormuz.[35] In general, the arbitration upheld the law of the sea and answered legal questions regarding the interpretation of UNCLOS. Future cases are now made aware of UNCLOS' ruling against historic claims to territory granting current rights to natural resources and exclusive economic zones. The ruling provides a legal framework for future negotiations and dispute settlements.[36] As such, future issues surrounding the Arctic, the Gulf of Mexico, and the Strait of Hormuz will have a precedent set that will help guide actions and negotiations in such a way that conflict and disputes may be avoided.

31. Phan and Nguyen, "South China Sea Arbitration," 49.
32. Friedman et al., "What Is the Future of the South China Sea?"
33. Gates, "International Law Adrift," 313.
34. Friedman et al., "What Is the Future of the South China Sea?"
35. Belding, "China's Island Building," 1019–25.
36. Phan and Nguyen, "South China Sea Arbitration," 50.

While the precedent set by UNCLOS may carry positive benefits for future cases, China's own actions will carry negative collateral effects. Without any punishment for China's actions, it is possible for other states to follow suit and begin ignoring UNCLOS Arbitral Tribunals.[37] China's goal in the SCS dispute is to isolate its opponents and force them into bilateral negotiations in an attempt to overpower each state individually and to assert sovereignty over the entirety of the SCS. To date, this has been an effective strategy for China and has resulted in great benefits, including the continuation of military and resources development.[38]

Unfortunately, China is not the first to ignore arbitrations through international courts or even from UNCLOS itself. Both Russia and the United States have a history of ignoring international courts, and Russia specifically set the precedent of ignoring ITL rulings during the Arctic Sunrise case. If powerful nations continue to set a precedent of rejecting findings from arbitrations that they find unfavorable, it will seriously reduce any incentive other states have of following their own unfavorable findings, and it may reduce the incentive for states to file resolutions in the first place.[39]

The United States' Ratification of UNCLOS

Currently, the United States is one of very few coastal states that has failed to ratify UNCLOS (also included are North Korea and Iran).[40] In fact, the United States is the only permanent member of the United Nations Security Council and the only North Atlantic Treaty Organization (NATO) member that is not a party to the Convention.[41] While there are a number of domestic political arguments for the United States' reluctance to ratify the treaty, the main reasoning is that even without the treaty its maritime rights and interests are upheld by the strength of its military, not through other agreements. Even after other states ratified UNCLOS, US navigational rights, water way access, and other maritime freedoms have not been impeded.[42]

37. Belding, "China's Island Building," 1027.
38. Castan, "Adrift in the South China Sea," 107.
39. Gates, "Adrift in the South China Sea," 318.
40. Friedman et al., "What Is the Future of the South China Sea?"
41. Shen Yamei, "United States: On Threshold of UNCLOS," (June 2015) *China International Studies* 52 (June 2015): 101.
42. Yamei, "United States," 105, 108.

However, US participation in UNCLOS could ensure future leadership and development of the law of the sea.[43] Ultimately, the ratification would result in an increase in credibility for the US and leadership by the US.[44] Specifically, in relation to the SCS dispute, US participation would allow for American jurists and legal scholars to participate in arbitrations and to influence and develop international maritime law.[45] For example, as a signatory to the Convention, the United States would be able to participate with the United Nations Commission on the Limits of the Continental Shelf and the International Seabed Authority. Organizations such as these are establishing legal systems for topics being disputed in the SCS.[46]

Beyond the United States' ability to participate in the creation of the legal framework of maritime law, as a member of the Convention, the US could also increase the credibility of the organization. If the US were to use UNCLOS to settle minor disputes between it and its immediate neighbors, such as Canada, US participation would improve UNCLOS' reputation as a legitimate organization with the authority to arbitrate between both great and small powers.[47] Through this legitimizing process, US membership within UNCLOS would likely result in a more powerful organization that would receive better responses from nations such as China. As has been mentioned, China's decision to ignore unsavory findings is not an isolated situation, and it is not the only powerful nation to do so; as such, while the United States may increase the legitimacy of UNCLOS, joining is not a concrete method to create better cooperation within the SCS.

Conclusion

This paper has analyzed the purpose and function of UNCLOS, using two examples of how the Convention has arbitrated disputes in the past, which demonstrates that UNCLOS has provided a successful dispute resolution mechanism. It has reviewed the background of the

43. Friedman et al., "What Is the Future of the South China Sea?"

44. Yann-Huei Song, "The U.S.-Led Proliferation Security Initiative and UNCLOS: Legality, Implementation, and an Assessment," *Ocean Development and International Law* 38, no. 1–2 (2007): 134, https://doi.org/10.1080/00908320601071421.

45. Gates, "International Law Adrift," 318.

46. Yamei, "United States," 102.

47. Gates, "International Law Adrift," 318.

China–Philippines SCS dispute and applied the UNCLOS decision to show that the Philippines has been wronged. It then examined the effects of the UNCLOS decision and how it will provide for reputational effects, but how UNCLOS has ultimately failed to reign in China's illegal and aggressive stance. Lastly, it posited that the United States' ratification of UNCLOS would increase the credibility of the organization, yet it would not reliably change China's actions. As a result, it is clear that US ratification would not assist in the SCS dispute, and regardless of UNCLOS' past successes, because of China's refusal to cooperate and UNCLOS' lack of an enforcement mechanism, UNCLOS has failed to resolve the SCS dispute.

Chasing Cyber-Supremacy: Securing US Military Dominance on the Battlefields of the Future

Brandon Amacher

Introduction

Throughout history, technological advancement has often turned the tide of military conflict and shifted power dynamics among nations. From the bow and arrow, to the advent of tanks and warplanes, technology has frequently proved a decisive factor in the outcome of war. The world is currently reaching a technological tipping point, and many have not even taken notice. For decades, cyber weapons have been developed and deployed right under many nations' noses. These weapons have been primarily used for the collection and dissemination of intelligence. However, we are now entering an era in which these virtual weapons can be used to cause conventional damage. Following the use of the Stuxnet virus to destroy Iranian nuclear centrifuges in 2013, former CIA and NSA director Michael Hayden compared the importance of the event to that of Hiroshima, saying, "This has the whiff of August 1945. . . . Someone, probably a nation state, just used a cyber weapon in a time of peace . . . to destroy what another nation could only describe as their critical infrastructure. . . . That's a big deal. That's never happened before."[1] Hayden recognized that this event had ushered in a new paradigm in warfare, the ramifications of which could not be ignored.

The world is entering a new age in which cyber weapons are being deployed alongside conventional weapons—an age in which the stroke of a keyboard could prove to be as lethal as the squeeze of a trigger.

1. Paul D. Shinkman, "Former CIA Director: Cyber Attack Game-Changers Comparable to Hiroshima," *US News & World Report* (February 20, 2013), https://www.usnews.com/news/articles/2013/02/20/former-cia-director-cyber-attack-game-changers-comparable-to-hiroshima.

The landscape of this cyber-hybrid battlefield is like nothing the world has seen before and is constantly evolving. The nations of the world will have to learn to adapt to this new frontier in combat, or be left behind. This paper will argue that in the age of cyber war, the United States should move to implement a combination of traditional and innovative tactics to maintain military dominance. This will be done by examining the history and development of cyber war and cyber weapons, assessing current threats and rival capabilities, and exploring potential tactics and solutions for the future.

Entering the Cyber Age: The History and Evolution of Cyber War

The history of modern computer science is inseparably linked with that of warfare. Alan Turing, the man widely known as the father of computer science, gained fame for his role in the cracking of Enigma, a Nazi means of encrypting communications. Turing and his associates at Bletchley Park used cutting edge tactics and computation machines to crack a cypher that was considered unbreakable at the time. This accomplishment not only validated Turing's methods, but also played a major role in bringing about the fall of the Axis powers. With regard to the intelligence obtained by cracking Enigma, Dwight D. Eisenhower said it "saved thousands of British and American lives and, in no small way, contributed to the speed with which the enemy was routed and eventually agreed to surrender."[2] From the inception of computing, the power of computers to influence outcomes in combat has been well-defined.

Until recently, a cyber war was considered a war over information. Computers were used to track, steal, disrupt, and decrypt enemy intelligence in order to support conventional military and government efforts. Recently, a new chapter in the story of cyber warfare has been opened, and it all started with one word: Stuxnet. As previously stated, the use of the Stuxnet cyber weapon[3] to destroy Iranian nuclear centrifuges showed the world that the increased integration of computers

2. Central Intelligence Agency, "The Enigma of Alan Turing," (April 10, 2015), https://www.cia.gov/news-information/featured-story-archive/2015-featured-story-archive/the-enigma-of-alan-turing.html.

3. It should be noted that no government has officially claimed responsibility for the Stuxnet attack though it is widely believed to have been a joint US–Israeli operation.

into critical systems had extended the capabilities of cyber-weapons beyond that of intelligence gathering. In this instance, malware was snuck onto Iranian computers and laid dormant until it was triggered, causing the centrifuges to spin at increasingly high speeds until they destroyed themselves. The nations of the world now had to take note, these weapons could now reach into the computers that control critical pieces of both military and civilian infrastructure and cause real damage. Despite this monumental shift, the idea of cyber war is still in its infancy, with many nations and decision makers not fully understanding the magnitude of the threat we now face.

The Ever-Changing State of Cyber War: Threats and Vulnerabilities

The state of cyber war is ever-changing, with new vulnerabilities and threats arising every day. Each of these has the potential to cause significant damage. The defense community is aware of the need to keep up with these threats, and it is working feverishly to do so. As Robert Ashley, the current director of the Defense Intelligence Agency (DIA) put it:

> In the coming year, we expect global cyberthreats to emanate from a wide array of state and nonstate actors. Our networks, systems, and information are at risk from an evolution of malicious cyberspace activities. . . . Our top adversaries are developing and using cyberspace to increase their operational reach into our military and civilian systems, exploiting our vulnerabilities, and compromising our national defense. Their capabilities will continue to challenge the adequacy of our current defenses and cybersecurity investments.[4]

For every advancement in computing, there are cases of both productive and malicious use. With the speed that these technologies are emerging, it seems nearly impossible to keep up. Although there are many such threats from innovation, this paper will focus on two of the most pressing: the Internet of Things, and quantum computers.

4. Robert Ashley, "Worldwide Threat Assessment," Defense Intelligence Agency (March 6, 2018), https://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/1457815/statement-for-the-record-worldwide-threat-assessment/.

The Internet of Things

Ironically, some of the nation's biggest vulnerabilities come in the form of very small devices. Over the last few years, the endpoints of many networks have changed from being either laptops or mobile phones, to tiny smart devices such as smart doorbells, smart thermostats, smart light bulbs, refrigerators, sensors, and many more. These millions of tiny devices comprise what is commonly known as the Internet of Things or, the IoT. The issue with these devices is that they are often designed with little to no regard for security. As the Department of Homeland Security put it:

> Unfortunately, IoT devices are often sorely lacking in security-focused features. These systems now offer the most attractive target to malicious actors, and are an increasingly large percentage of the devices in the ecosystem. In fact, the November 2016 Ericsson Mobility Report predicted that IoT devices will surpass mobile phones as the largest category of connected devices in 2018. Given the level of security on IoT devices, that is a daunting prediction.[5]

Some may think these devices are too small to present a significant threat, but, as Director Ashley puts it, "The most important emerging cyberthreats to our national security will come from exploitation of our weakest technology components: mobile devices and the Internet of Things."[6] These devices pose a major threat for two reasons: they can provide an open access point to the other network components upstream, and they can be used en masse for botnet attacks.

Large components of networks, such as servers, are often locked down tight with security measures such as firewalls and heavy encryption, but these servers reside on the same network as small, unsecured IoT devices, which are considered trusted members of the network. This allows hackers who compromise these IoT devices to gain access to the rest of the network and do real harm. In august 2019, Microsoft released a report that Russian-state-backed hackers have been using

5. US Department of Commerce and US Department of Homeland Security, "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," (May 22, 2018), https://www.commerce.gov/sites/default/files/2018-06/eo_13800_botnet_report_-_finalv2.pdf.

6. Robert Ashley, "Worldwide Threat Assessment."

this very vulnerability to breach secure networks.[7] One case that illustrates how impactful such breaches can be is the 2013 Target data breach. Hackers were able to gain access to Target's secure network through a smart heating and air-conditioning control unit. Once they gained deeper access into Target's systems, they were able to extract 11 GB worth of data containing approximately 70 million records.[8] Target initially stated, in their 2013 10-K, that they would incur $61 million in expenses related to the data breach. After a few years and over 140 lawsuits later, their 2016 10-K stated, "since the Data Breach, we have incurred $292 million of cumulative expenses, partially offset by insurance recoveries of $90 million, for net cumulative expenses of $202 million."[9] The costs detailed by Target in their annual reports are just the tip of the iceberg when looking at the complete cost of their massive data breach. Target actually incurred costs ranging from $1.76 billion to $2.50 billion, 2.4–3.4% of their total revenue and 89%–127% of their net income in 2013.

Total of Cost incurred ($)	Best Case	Worst Case
Data-Breach Related Expenses	292,000,000	292,000,000
Q4 2013 Decline in Rev.	1,319,448,088	1,709,762,362
Q1 2014 Decline in Rev.	208,000,000	411,868,140
Cost of Losing CEO	25,800,000	82,400,000
Cost of Losing CIO	2,000,000	4,000,000
Total (with insurance)	**1,757,248,088**	2,410,030,501
Total (without insurance)	1,847,248,088	**2,500,030,501**

Target stated, "We know our guests' confidence in Target and the broader US payment system has been shaken."[10] The impact of the loss

7. Zak Doffman, "Microsoft Warns Russian Hackers Can Breach Secure Networks Through Simple IoT Devices," *Forbes* (August 5, 2019), https://www.forbes.com/sites/zakdoffman/2019/08/05/microsoft-warns-russian-hackers-can-breach-companies-through-millions-of-simple-iot-devices/?sh=bceae84617ff#770184e6617f?&web_view=true.

8. Maggie McGrath, "Target Data Breach Spilled Info on As Many as 70 Million Customers," *Forbes* (January 14, 2014), https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/?sh=5f413a3ce795.

9. United States Securities and Exchange Commission (SEC), "Form 10-K: 10-K Report: Target 2016 Annual Report, https://corporate.target.com/annual-reports/2016/10-K/form-10-K.

10. SEC, "Form 10-K: 10-K Report: Target 2013 Annual Report, https://sec.report/Document/0000027419-20-000008/.

in confidence resulted in a decline of $1.5-$2.1 billion in revenue from Q3 (2013) and Q1 (2014).[11,12] Moreover, the board of directors decided to remove their current CEO and CIO, resulting in a probable cost of replacement of 200–400% of their annual salaries. This resulted in a cost range of $27.8–$86.4 million to adequately replace these C-suite executives.[13] This is just one example of how one unsecured IoT device can lead to the loss of millions of records and billions of dollars.

The second reason that IoT devices present such a threat is the fact that thousands to millions of these devices can be hijacked, and their combined processing power can be used to attack and take down large targets in an event known as a "botnet." These botnets have a surprising amount of computational power and have even been able to take down major sites for hours or days at a time. For example, in 2016, the Mirai botnet took down several high-profile targets such as Twitter, Netflix, Reddit, and GitHub by using the combined power of approximately 400,000 IoT devices in a distributed denial-of-service attack (DDoS.)[14] Since this attack, the Mirai malware and others have been used to perpetrate several other attacks. With the deployment of less secure IoT devices every day, these occurrences are likely to occur more often and with an increased level of severity. Nation-states could easily perpetuate these attacks in order to deal a severe economic blow to an adversary. The unsecured growth of the IoT represents a significant vulnerability to the US's cyber defense.

Quantum Computers

Another advance in technology with serious implications in cyber warfare is the development of quantum computing. Quantum computers are a revolutionary combination of computer science and quantum mechanics. These futuristic machines use the quantum states of sub-

11. SEC. "Form 10-Q: 10-Q Report for the Quarterly Period Ended November 2, 2013, Target 2013 Quarterly Report, https://www.sec.gov/Archives/edgar/data/27419/000002741918000010/tgt-20180203x10k.htm.

12. "Form 10-Q: 10-Q Report For the quarterly period ended May 4, 2014 Target 2013 Quarterly Report," https://www.sec.gov/Archives/edgar/data/27419/000002741914000014/tgt-20140201x10k.htm.

13. "The Impact of Losing an Executive," *Chief Executive,* October 20, 2016, https://chiefexecutive.net/impact-of-losing-an-executive/.

14. Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer* 50, no. 7 (2017): 80–84. https://doi.org/10.1109/mc.2017.201.

atomic particles in place of traditional bits for processing data. These quantum bits, or "qubits," enable quantum computers to process massive amounts of information in a very short period of time. For example, a joint Google/NASA quantum computer prototype recently achieved what is known as "quantum supremacy," meaning that their quantum computer was able to solve a complex math problem in a few seconds that would have taken the best supercomputer in the world thousands of years to complete.[15]

This breakthrough has serious security implications due to the fact that this ability to solve complex problems very quickly would also allow quantum computers to break traditional encryption standards. This essentially means that if someone were to have a viable quantum computer, they could decipher and read nearly all internet traffic up to and including, financial records, usernames and passwords, government transmissions, and other vital classified information.[16] This paper has already discussed the impact that the ability to decipher Enigma had on the outcome of the Second World War, and quantum computers could very well yield a similar condition, but with access to an exponentially larger amount of data. This is especially concerning when one takes into account the massive amount of investment that China has put into quantum computing technology, which has allowed them to take a lead in many areas of the field.[17] Should China develop quantum technology before the US, it is likely that this would lend them a significant military and economic advantage, and perhaps even give China a net advantage on the world military stage.

The Cyber Battlefield of Today: The Capabilities of Geopolitical Rivals

The US military possesses the most powerful conventional military on earth. The US has a larger and superior air force to any other nation,

15. Frank Tavares, "Google and NASA Achieve Quantum Supremacy," NASA, October 23, 2019, https://www.nasa.gov/feature/ames/quantum-supremacy/.

16. Steve Jurvetson, "How a Quantum Computer Could Break 2048-Bit RSA Encryption in 8 Hours," *MIT Technology Review*, May 30, 2019, https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.

17. Paul Smith-Goodson, "Quantum USA Vs. Quantum China: The World's Most Important Technology Race," *Forbes*, October 10, 2019, https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/?sh=3f1f19f372de.

a far better navy, and spends more than double on defense than any other nation.[18] For any other nation-state, taking on the US military head to head would be extremely costly and unappealing. For this reason, the United States' foes would not likely undertake straightforward warfare, and would instead opt to implement an asymmetric strategy. Asymmetric warfare is the application of tactics that deviate from the norm in order to avoid an enemy's superior strengths and apply their own strengths in a way that levels the playing field. Former US Army General David L. Grange describes the situation as follows:

> Because no group or state can defeat the U.S. in conventional warfare, America 's adversaries and potential adversaries are turning to asymmetric strategies. We must therefore understand asymmetric warfare, and be able to respond in kind. . . . Wars were primarily fought by nation-states with balanced, conventional fighting capabilities. When asymmetric methods were used, usually in the form of maneuver or technological advantage, they had a dramatic effect.[19]

The use of cyber weapons as part of an asymmetric strategy should be a major concern for US military strategists looking forward, particularly with reference to near peers such as Russia and China. Both of these countries have been actively developing significant offensive and defensive cyber capabilities.

Russia

Russia has been actively implementing cyber weapons and cyber war to achieve its political goals. President Vladimir Putin has made the development and implementation of cyber weapons one of his top priorities as president. As Jeffery Carr, a leading cybersecurity analyst and founder of Project Grey Goose, puts it in his book, "The Russian Federation's cyber posture was one of President Putin's highest priorities after taking office in December 1999. As a result, Russia probably has the most coherent state plan integrating private and government

18. Ellen Ioanes, "These Are the 25 Most Powerful Militaries in the World in 2019," *Business Insider*, September 27, 2019, https://www.businessinsider.in/defense/these-are-the-25-most-powerful-militaries-in-the-world-in-2019/articleshow/71340757.cms.

19. David L. Grange, "Asymmetric Warfare: Old Method, New Concern," *National Strategy Forum Review*, 2000, https://www.scribd.com/document/49206217/Asymmetric-Warfare-Old-Method-New-Concern.

cyber sectors."[20] The Russians have been aggressive in their efforts to use cyber weapons both to control the flow of information and to augment their already formidable military forces. Some of the information warfare conducted by the Russians includes the interference in foreign elections and the stealing and leaking of classified documents. These hacks are often focused on government and government affiliated organizations, such as political parties and think tanks. These attacks have even reached the US and some of our closest allies, with Russian hackers having been caught attempting to steal information from both US and EU non-governmental organizations (NGOs) and think tanks in 2019.[21,22]

Perhaps even more daunting are the Russian cyberattacks that are intended to compromise critical infrastructure. The best example of this can be seen in Ukraine. Since 2014, Russia has launched a near-constant barrage of cyberattacks on its neighbor. Hackers have ravaged the Ukrainian power grid, causing frequent widespread blackouts. This was done by placing malware on several computers within at least three major Ukrainian power companies.[23] This malware can lie dormant for months at a time until it is triggered at the behest of the hacker, often during storms or other adverse circumstances to cause maximum damage and disruption.[24] Although these attacks have almost exclusively been used in Ukraine, the Russians have also been found to have these weapons in place inside of the critical infrastructure of other nations, including the United States. Hackers had been found to have infiltrated more than 20 power companies, including several within the US, and were able to obtain a high level of access. Andy Greenburg describes this as follows:

20. Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, (Sebastopol, CA: O'Reilley), 217.

21. Dustin Volz, "Russia, Iran, North Korea Launch Hundreds of Cyberattacks on U.S. Political Groups, Microsoft Says," *The Wall Street Journal*, July 18, 2019, https://www.wsj.com/articles/russia-iran-north-korea-launch-hundreds-of-cyberattacks-on-u-s-political-groups-microsoft-says-11563397201.

22. Lucas Laursen, "Russia-Linked Hackers Responsible for Vast European Cyber Attacks, Says Microsoft," *Fortune*, February 20, 2019, https://fortune.com/2019/02/20/microsoft-russia-hacking-europe/.

23. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, April 13, 2018, https://www.wired.com/story/russian-hackers-attack-ukraine/.

24. Greenberg, "How An Entire Nation."

> Forensic analysis found that the hackers obtained what they call operational access: control of the interfaces power company engineers use to send actual commands to equipment like circuit breakers, giving them the ability to stop the flow of electricity into US homes and businesses.[25]

These findings are evidence of the fact that not only is Russia capable of conducting similar cyberattacks on US soil, but also that they are ready and willing to do so in the case of a conflict.

China

China has been an active participant in the creation and usage of hacking groups for some time. Since 2002, the Chinese government and the People's Liberation Army (PLA) have been very focused on creating and deploying hacking groups primarily focused on being able to take down enemy communications systems in a quick coordinated attack.[26] In order to accomplish this end, the PLA has created information warfare militia units especially dedicated to this task. These units consist of a blend of personnel from the Military, Government, and the private sector.[27] This blend of industry with government provides China with a strategic advantage. This allows the authoritarian Chinese government to dictate the actions of the ever-growing Chinese tech industry and have a hand in the development and deployment of their products.

China has already used its large tech companies to conduct cyber espionage; the most infamous example of this being the alleged use of Huawei devices, such as telecommunications infrastructure and cellphones, to conduct espionage on behalf of the Chinese government. The US government has been suspicious of Huawei for years, and mounting evidence confirming these suspicions has led to the complete ban on the importation of Huawei devices to the US.[28] The belief among top government officials is that the Chinese government in-

25. Andy Greenberg, "Hackers Gain Direct Access to US Power Grid Controls," *Wired*, September 6, 2017, https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/.

26. Carr, *Inside Cyber Warfare*, 258.

27. Carr, *Inside Cyber Warfare*, 256.

28. David Shepardson, "Huawei, ZTE 'Cannot Be Trusted and Pose Security Threat: U.S. Attorney General," *Reuters*, November 14, 2019, https://www.reuters.com/article/us-usa-huawei-tech-zte/huawei-zte-cannot-be-trusted-and-pose-security-threat-u-s-attorney-general-idUSKBN1XO2UJ.

tends to use Huawei devices to carry out their goal of disrupting communications networks. On this topic, Federal Communications Commission (FCC) Chairman Ajit Pai said, "[The commission] cannot ignore the risk that the Chinese government will seek to exploit network vulnerabilities in order to engage in espionage, insert malware and viruses, and otherwise compromise our critical communications networks."[29] This incident is not unprecedented either, with several other security breaches being found on Chinese devices, including compromised security cameras, having been found in the recent past.[30]

China is notorious for stealing and reproducing intellectual property. This theft ranges from commercial products to military technology. China has likewise deployed this tactic on the cyber battlefield. In 2016, Chinese hackers were discovered to have stolen several NSA cyberweapons and used them against the U.S. and its allies.[31] The Chinese are actively looking to steal and use whatever information or technology they can from the United States' cyber efforts. Additionally, the government of China has begun probing cyber vulnerabilities in the critical infrastructure of the US, much like their Russian counterparts.

The Doctrine, Tactics, and Attitudes of Cyber-Dominance

Perhaps the most problematic issue in the perceptions of many toward cyber threats lay in their lack of understanding of just how significant and potentially devastating a cyberwar could be. The digital revolution we are currently experiencing is changing the world more profoundly than any event since the industrial revolution. Just as industrialization changed warfare forever with the advent of mass production of machine guns, tanks, and combat aircraft, the digital revolution is in the process of changing the very nature of international combat. Every future war will in all likelihood now include a cyber component and the effective use of cyber weapons may prove a deciding factor. As technology advances, military doctrine and tactics must adapt as well,

29. Shepardson, "Huawei."

30. Zak Doffman, "Warning as Millions of Chinese-Made Cameras Can Be Hacked to Spy on Users: Report," *Forbes*, August 2019, https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/?sh=2c8e931d6bf2.

31. Nicole Perlroth, David E. Sanger, and Scott Shane, "How Chinese Spies Got the N.S.A.'s Hacking Tools, and Used Them for Attacks," *The New York Times*, May 6, 2019, https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html.

or a military may find itself metaphorically forming a firing line in front of a cyber Gatling-gun. The United States must be proactive in adapting these tactics in order to maintain its dominance. The following sections discuss some changes, strategies, and tactics that could help the United States succeed on the cyber battlefield.

Knocking Down Barriers

A shared trait among America's major cyber rivals is the blended nature of their cyber war effort. In both Russia and China, the lines between the government, private sector, and academia are blurred, bordering on nonexistent. The authoritarian nature of these regimes allows them to influence the actions of academics and corporations to a much higher degree than in the United States. This is clearly evident with Huawei in China. Both of these nations often carry out their cyber-attacks through non-government hacking syndicates in order to attain a level of plausible deniability. Additionally, school and university systems in these nations are geared directly at indoctrinating students and engendering loyalty to the regime. The *Encyclopedia Britannica* describes the Chinese education system as "a major vehicle for both inculcating values in and teaching needed skills to its people."[32] Many Chinese hackers are sent to military school before being given jobs in the Chinese private sector in order "to nationalize and promote loyalty within the warriors."[33]

Additionally, the US education system is not nearly as integrated into the cyber war effort as the Chinese and Russian systems are. The United States education structure, particularly the university system, are far more separated from the control of the central government, in large part due to the emphasis placed on academic liberty. The US government does, however, recognize the value of the research and resources that academia has to offer. For this purpose, the NSA has designated certain universities renowned for their prowess in computer science and mathematics as "NSA centers of excellence." While this may be a step in the right direction, these efforts have also been criticized for being limited in their purview to primarily recruiting engineering talent from these institutions. Professor Jan Kallberg of the University of

32. Benjamin Elman and Kenneth G. Lieberthal, "Education," *Encyclopædia Britannica*, November 2019.

33. Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, (Sebastopol, CA: Ryley Media, 2009), 257.

Texas presents the following critique:

> The future will require cyber defense research teams that can address not only computer science, electrical engineering, and software and hardware security, but also political theory, institutional theory, behavioral psychology, deterrence theory, military ethics, international law, international relations, and additional social sciences. Researchers working alongside DOD to develop tool sets for information operations as a subset of cyber operations, utilizing social media and exploiting collective behavior, would require a broad mix of social science and behavioral psychology competencies.[34]

The need for increased cooperation between government, industry, and academia may prove crucial to the ongoing efficacy of American cyber capabilities. In order to foster this cooperation, the government should strongly consider the creation and funding of cyber consortiums that could bring these sectors together. Additionally, the government should allow these organizations to aid in the collection and analysis of open source intelligence and even, when appropriate, processing security clearances for members so that they can more effectively help solve pressing national security issues. As cyber war becomes more prevalent, the United States will require a greater number of our best minds to stay competitive. The proper use of human and technical resources may very well make or break the American cyber war initiative.

Cyber Blockades

Blockades are an age-old economic warfare tactic used to deny an enemy access to goods or services outside of their borders. Historically, blockades have typically been naval operations where a naval force disallows enemy merchant ships from entering or leaving port. A cyber blockade puts a modern twist on this traditional tactic. The idea of a cyber blockade is described as follows:

> Cyber blockade is a situation rendered by an attack on cyber infrastructure or systems that prevents a state from accessing cyberspace, thus preventing the transmission (ingress and egress) of data beyond a geographical boundary. Cyber

34. Jan Kallberg, "Cyber Operations—Bridging from Concept to Cyber Superiority," *Joint Forces Quarterly*, 68 (2013): 58.

> blockades carry the potential to inflict political, economic, military, and social damage on the target state, and can be considered acts of war.[35]

The efficacy of a cyber blockade is largely dependent on the ability of the attacking nation to deny access to critical points on the internet. In this respect, the power of the United States is unmatched. The internet originated as a project of DARPA, an advanced technology research branch of the US Department of Defense. Until recently, the United States had direct control over the backbone of the internet with its control of Internet Corporation for Assigned Names and Numbers (ICANN), an organization that oversees the assignment of IP addresses, network protocol assignments, and many other crucial internet functions.[36] The decision to privatize this organization has been controversial, and many believe that the US should reclaim control of the corporation. Nevertheless, the United States' level of control over the internet remains unrivaled by any other nation. The United States is home to eight of the ten largest internet companies in the world, including Amazon, Apple, Microsoft, and Google, which dwarf the rest of the pack.[37] Amazon web services alone claims 40% of the cloud hosting market.[38] The ability of the government to compel these companies to sever ties with adversarial governments in the case of a US-imposed cyber blockade would deny access to broad swaths of the internet and severely damage the economy of any developed or semi-developed nation.

A cyber blockade such as this could prove just as disruptive as a traditional one. As Alison Russell puts it:

> Cyber blockades and traditional blockades have similar effects on society. In both cases, society is denied access to

35. Alison Lawlor Russell, *Cyber Blockades*, (Washington DC: Georgetown University Press, 2014), 5.

36. Mark Grabowski, "Should the U.S. Reclaim Control of the Internet? Evaluating ICANN's Administrative Oversight Since the 2016 Handover," *Nebraska Law Review,* August 6, 2018, https://lawreview.unl.edu/Should-the-U.S.-Reclaim-Control-of-the-Internet%3F.

37. "Top Internet Companies: Global Market Value 2019," *Statista*, https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/.

38. Russell Brandom, "Using the Internet without the Amazon Cloud," *The Verge*, July 28, 2018, https://www.theverge.com/2018/7/28/17622792/plugin-use-the-internet-without-the-amazon-cloud.

> goods and information that it normally accesses. This imposed denial of access reduces economic productivity and engenders frustration and uncertainty in society, since it is usually not known how long the denial will last and how routine business will be interrupted. This uncertainty creates fear and psychological distress in society, particularly if the cyber blockade occurs during a crisis that makes access to the information more important. Thus, the interruption of routine transactions for an unknown period of time occurs in both traditional and cyber blockades, creating fear and uncertainty in society.[39]

The use of a cyber blockade could prove to be one of the United States' greatest resources in case of a cyber war and would likely create a disproportionately large impact when compared to the cost thereof.[40] Due to these unique advantages, the US should prepare battle plans that include the implementation of cyber blockades.

Cyber Alliances

The enactment of alliances is as old as warfare itself. These partnerships and organizations have evolved over time and are currently undergoing a period of great change to adapt to the rising challenge of cyber war. The internet provides such a level of interconnectivity that it essentially supersedes borders. In this world of unprecedented connection, cooperation with allies is more important than ever. A cyber attack on one ally would have major implications on both the economic well-being and safety of other allies. For this purpose it is essential that cyber defense plans and practices be established with allies and treaty organizations. Some cyber alliances and organizations are already in place. Organizations such as Five Eyes are primarily focused on surveillance, a crucial component of cyber war, but as cyber warfare evolves, this may not be enough. Alliances will have to adapt in order to implement offensive responses and tactics into their strategic plans.

NATO is one organization that has recognized this need and has adopted cyber-operations as one of their core objectives. As their website puts it:

> Cyber threats to the security of the Alliance are becoming more frequent, complex, destructive and coercive. NATO

39. Russell, *Cyber Blockades*, 137.
40. Russell, *Cyber Blockades*, 137.

> will continue to adapt to the evolving cyber threat landscape. NATO and its Allies rely on strong and resilient cyber defenses to fulfil the Alliance 's core tasks of collective defense, crisis management and cooperative security. The Alliance needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces.[41]

This recognition of need is a step in the right direction; however, the United States and its allies must beware of adopting a reactive mindset when it comes to cyber threats as opposed to a proactive one. The time to prepare for a cyber war is before one actually breaks out and US alliances should prepare and be ready to deploy offensive measures (such as cyber blockades) in addition to the current monitoring of threats and defensive stratagems.

Because the US is typically very tight lipped about its offensive cyber operations, it is difficult to assess the extent to which offensive capabilities with allies have been developed. Although no nation has officially claimed responsibility, it is widely believed that the Stuxnet weapon used to destroy Iranian nuclear centrifuges was a joint US–Israeli operation.[42] Hopefully, the United States will continue to pursue the development of these programs and weapons alongside her allies in order to maintain influence and mutual security.

Conclusion

The magnitude of the change wrought on the modern battlefield by the digital revolution cannot be taken lightly. Cyber warfare will likely play a role in every major military conflict going forward, and as time passes this role will only become more important. As technology progresses, new threats emerge. The United States' rivals recognize the importance of this new frontier in battle and hope to utilize asymmetric strategies to overcome the might of the American military. Russia and China are actively developing, testing, and deploying cyber weapons to reach their geopolitical ends; additionally, these two nations and more are constantly probing for weaknesses in American cyber industry. The US must stay at the forefront of computing technology and be responsible in its deployment of new technologies, such as the Internet

41. NATO, "Cyber Defence," NATO, October 2019.

42. Ralph Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy* 9, no. 3 (2011), 49–51, .https://doi.org/10.1109/MSP.2011.67.

of Things and quantum computers, in order to avoid being vulnerable to potentially devastating attacks from these and other malicious actors.

Despite the efforts of America's foes to exploit cyber war as a weakness, the United States could be the most formidable cyber power on earth due to its unique influence in the development and control of the internet and computational technologies. In order to attain this end, the United States will have to be willing to adapt quickly and view these threats and opportunities in a new way. For instance, Russia and China both take advantage of the authoritarian nature of their regimes in order to tap the resources of their private and academic sectors to contribute to their cyber war effort. In order to remain the supreme military power in this age, the US will need to become a more dynamic, highly adaptive cyber power with a high level of cooperation between public, private, and academic spheres. Furthermore, the US must be willing to adopt new tactics and adapt existing tactics in order to stay competitive. The use of cyber blockades and the existence of robust alliances for mutual cyber defense may prove crucial in keeping the world safe against hybrid conventional/cyber aggressions. The United States must move to implement a combination of traditional and innovative tactics to maintain military dominance. The level of success in doing so may determine whether freedom or tyranny take the front seat in the global politics of the future.

The Application of the Law of Armed Conflict in Space

Cash D. Holdaway

A note from the author: This paper was written while the United States Space Force was being established as a new branch of the United States Military; this paper in no way was influenced by this action and would have been written in the same fashion as if such a thing never existed.

Almost thirty years have passed since the Cold War came to a somewhat peaceful end. During the forty-four years of conflict, tensions often skyrocketed, and threats of nuclear devastation were constant. The mutually assured destruction that existed between the Soviet Union and the United States stabilized the world and perhaps even prevented World War III. What would happen, conversely, when states move away from nuclear abilities and technology, and instead invested in other means of which to infiltrate, sabotage, and undermine foreign governments? This question is more than just a theory—it is today's reality.

The power struggle between the United States and the Soviet Union and their goal to reach space in the mid-1950s to the 1970s is often referred to as the Space Race. However, it may be argued that the real space race is continuing to take place today as our technologies are rapidly advancing and our capabilities greatly exceed merely placing a man on the moon. Today, the capabilities of the United States and its enemies are far more dangerous and could potentially be the key to worldwide power and authority for whoever succeeds in wielding the superior technology. Terrestrial conflicts are now being fought in space which beg the questions, is the United States prepared for a conflict in space? How is the United States going to react to both kinetic and non-kinetic attacks in space? Most importantly, what are the legal authorities and parameters that exist regarding armed conflict in space?

These questions must be answered for the United States to compete with the rising powers that threaten democracy and the American way of life.

From the bow and arrow to intercontinental ballistic missiles, newly developed technologies have been weaponized to make their mark on the battlefield and lawmakers and citizens alike have questioned the legality and ethics of these technologies being used in combat. From the invention of firearms, to nuclear warheads, and now cyberattacks, and kinetic capabilities (anti-satellite (ASAT) missiles) in space, the public and governments have questioned the humanity and validity of the use of new technologies. In order to form proper rules of engagement to a kinetic or non-kinetic attack in space that is consistent with the law of armed conflict, legislators can look towards the law and policy that is applicable to maritime operations[1] and cyber operations[2] which can be relatable to this new domain of combat.

As a response to the atrocities of WWII, the UN Charter was signed into treaty on June 26, 1945, at the United Nations (UN) conference in San Francisco shortly following the end of the war.[3] The Charter contains rules, regulations, and restrictions for signatory states in order to prevent further conflicts. For example, Article 2(4) prohibits belligerency between states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[4] The only three exceptions to this rule are as follows: Article 51 of the UN Charter (Self Defense), a unanimous decision of the United Nations Security Council (UNSC), or the consent of the opposing state.[5]

The purpose of this paper is to articulate a legal framework following the guidelines set for any international armed conflict by the

1. Law of the Sea Library, *The Law of the Sea, a Select Bibliography* (New York: Office of the Special Representative of the Secretary-General for the Law of the Sea, annual publications).

2. Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

3. "Charter of the United Nations," United Nations, accessed November 18, 2019, https://www.un.org/en/charter-united-nations/.

4. "Repertory of Practice of United Nations Organs," United Nations, accessed November 18, 2019, http://legal.un.org/repertory/art2.shtml.

5. "Repertory of Practice of United Nations Organs," United Nations, accessed November 18, 2019, http://legal.un.org/repertory/art51.shtml.

Geneva and Hague Conventions and the UN Charter, in the event that either a kinetic or non-kinetic attack occurs on the sovereignty of the United States in the space domain. This will not be a simple answer, however, since complicated differences exist between terrestrial-based attacks, cyber-based attacks, and attacks in space on either military or civilian objectives.

Under Article 2(4) of the UN Charter, any attack on a state's territory or sovereignty from another state, unless authorized by the UNSC or either defending itself or consenting to the use of force, is a belligerent action and is against the law of armed conflict. There are existing treaties regarding space and international law, but there is no concrete law or policy regarding the law of armed conflict in the application of the space domain. To comprehend how the law of armed conflict applies in space, one must understand what kind of resources governments and civilian corporations have orbiting Earth's atmosphere and what kind of effect that threats on these resources have on national security.

Capabilities and Resources in Space

According to the Union of Concerned Scientists (UCS), 2,218 operational satellites are currently in orbit. Of those, the United States has 1,007, far more than China who has the second most satellites in orbit at 323, followed by Russia at 164. Of the 1,007 US satellites, 35 are civil, 620 are commercial, 164 are government and 189 are military.[6] These satellites that are operated by the United States and rival countries have many functions and orbit at different levels based on those functions. An article released by the Defense Intelligence Agency outlines the capabilities performed by U.S. satellites. These types and functions will be analyzed below.[7]

Types and Functions of Satellites

There are four types and functions of satellites that affect national security and defense. The several capabilities that the various satellites in operation perform are communication, intelligence, surveillance,

6. "UCS Satellite Database," Union of Concerned Scientists, March 31, 2019, https://www.ucsusa.org/resources/satellite-database.

7. *Challenges to Security in Space*, Defense Intelligence Agency, January 2019, 8, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

and reconnaissance (ISR), missile warning, and position, navigation, and timing (PNT). These capabilities will be further broken down.

Communication Satellites

Communication satellites are satellites used by the government, the military, civilians, or commercial businesses to provide voice communication, broadcast television, internet broadband, mobile services, and data transfer worldwide.[8]

ISR

Satellites that have intelligence, surveillance, and reconnaissance capabilities support military objectives by collecting a broad range of intelligence in order to support the mission of the military and government. Civil and commercial ISR satellites collect information regarding the Earth's land, sea, and air for research purposes.[9]

Missile Warning

Missile warning provides the first line of defense for the United States. It has the ability to immediately detect the launch of a foreign state's missile and where it will detonate. Ground-based radar provides follow up information to confirm the attack.[10]

PNT

Position, navigation, and timing (PNT) functions in a satellite constellation allow precise location and timing services to reach the entire globe. Both civilian and military consumers use these abilities to navigate and locate their objectives.[11]

It is easy to see how these capabilities could be targeted by foreign belligerent actors. It must be understood the importance of each type of satellite and what the collateral damage will be in the event of an attack. In the context of war in space, it will most certainly, at this point in time, be an international armed conflict (IAC) involving any two sovereign states. While it is hard to find concrete evidence that belligerent non-state groups such as the Islamic State (ISIS) or Al-Qaeda have capabilities in space, a Washington Post report in 2013[12] shows that

8. *Challenges to Security in Space*, 8.

9. *Challenges to Security in Space*, 8.

10. *Challenges to Security in Space*, 8.

11. *Challenges to Security in Space*, 8.

12. Craig Whitlock and Barton Gellman, "U.S. documents detail al-Qaeda's efforts to fight back against drones," *The Washington Post*, September 3, 2013,

Al-Qaeda was developing the technology to interfere with U.S. GPS signals which is a great concern for the United States.[13] Concern should also be given to the possibility of certain states who sponsor terrorism to aid in the mission of those terrorist groups whose best interest it is to possess this advanced technology in order to harm western states. In that situation, however, the circumstances may still classify the conflict as an IAC.

For the purpose of this paper, focus will be given to the four countries that are the most threatening to the United States at the time of this publication: Russia, China, North Korea, and Iran (known in the US national security community as the 2+2). Russia and China have already attacked the United States in cyberspace, and debate is still ongoing on how the United States should react to attacks in cyber and in US institutions, such as the Russian infiltration of the 2016 presidential election.[14] According to the DIA, Iran and North Korea do not pose the same level of threat as Russia or China, however, both have non-kinetic capabilities that can be used against the United States, and North Korea has ballistic missiles that could theoretically reach orbit and threaten US resources.[15] These threats need to be taken into account when constructing laws and policy regarding reactionary advances.

Sovereignty in Space: From Naval Ships to Spaceships

Before one can determine the legality of any type of attack in space during war, it must be defined what constitutes sovereignty in space. As technological advancements occurred, moral and legal questions also evolved into what we know and reference today such as was decided in the Geneva and Hague conventions and the UN Charter. The idea of sovereignty in the areas known as global commons, or international territory that is not technically owned by any state, has been challenged before; for example, certain areas of Antarctica and the Senkaku

https://www.washingtonpost.com/world/national-security/us-documents-detail-al-qaedas-efforts-to-fight-back-againstdrones/2013/09/03/b83e7654-11c0-11e3-b630-36617ca6640f_story.html?utm_term=.c15349e5bf7b.

13. "Space Threat 2018: Other Actors Assessment." *Aerospace Security*, February 28, 2019, https://aerospace.csis.org/space-threat-2018-other-actors/.

14. 116th Congress, *Report of the Select committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, July, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

15. *Challenges to Security in Space*, 13–32.

Islands in the East China Sea are frequently being disputed as to which state that area belongs to. Today there are many laws constructed around crimes committed in the global commons which can be used as a guide when analyzing threats in space. The high seas, along with space, is one of the largest areas in which international crime is committed, and as such, has many laws governing the process of prosecution. For example, if a crime is committed in international waters on a private shipping vessel that is owned by a US company, then they will be prosecuted in the United States. Until then, the captain of the ship has full authority.[16] The same can be applied to an attack in outer space by a foreign state or entity on a US-owned private satellite, such as a Verizon communication satellite. The United States should be able to prosecute whoever conducted the attack.

Principles of the Law of Armed Conflict

Before discussing the possibility of conducting either a primary or retaliatory attack, one must understand the four guiding principles that state whether the attack would be legal. These four principles stem from the law of armed conflict and relating policy and are: military necessity, distinction and discrimination, proportionality, and humanity or unnecessary suffering.

For the target objective to qualify as a legal target, it must be provisioned that the elimination of such objective is necessary in order to promote mission success of the state's military. In legal terms this is known as military necessity. This is outlined in the UN Charter under Article 52 of Additional Protocol I (API), which allows for the targeting of certain individuals or physical objects to be legal under the principle that those specific targets pose a threat to the success of the mission.[17]

Article 48 of API of the UN Charter defines discrimination and distinction as "distinguish[ing] between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." This

16. "Crime Aboard High Seas," FBI Retired, accessed December 12, 2019, https://fbiretired.com/skillset/crime-aboard-high-seas/.

17. *Law of Armed Conflict Documentary Supplement* (Charlottesville, VA: International and Operational Law Department, the United States Army Judge Advocate Generals Legal Center and School, 2012), 211–12, https://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Documentary-Supplement-2012.pdf.

clearly states that civilian lives or property cannot be damaged or harmed unless otherwise involved in belligerent behavior.[18]

Proportionality is an important principle to account for when targeting an objective. Under Article 52 of API of the UN Charter, proportionality is defined as any damage to civilian life or property that is "excessive in relation to the concrete and direct military advantage anticipated." This also counts as an indiscriminate attack which is also prohibited under Article 52.[19]

The principle of humanity protects combatants from experiencing unnecessary suffering. Even though war may be unavoidable, these laws were set in place to prevent combatants from suffering from inhumane methods of war that were practiced in WWI and WWII among others. This principle can be found in Article 35 of API.[20]

Kinetic Threats

As of 2019, both Russia and China have been in the process of developing anti-satellite (ASAT) capabilities to destroy satellites in low Earth orbit (LEO) where both communication and ISR satellites orbit. North Korea theoretically also has this capability while Iran does not.[21] The United States must prepare for an attack by a state with these capabilities while keeping congruent with the international laws set in place by the UN charter. As stated above, three possible scenarios will be examined based on kinetic threat capabilities.

Scenario One: State A Directs Kinetic Attack on State B Military/Government Satellite.

When a state conducts a cyberattack, it is usually very difficult to ascertain where the attack originates from.[22] When a state launches a missile to destroy a satellite, however, it is usually clear who initiated the

18. "Treaties, States parties, and Commentaries: Additional Protocol (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977," International Committee of the Red Cross, accessed December 13, 2019, https://ihl-databases.icrc.org/ihl/WebART/470-750061?OpenDocument.

19. *Law of Armed Conflict Documentary Supplement*, 211.

20. *Law of Armed Conflict Documentary Supplement*, 207.

21. *Challenges to Security in Space*, 31–32.

22. Larry Greenemeier, "Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers," *Scientific American*, June 11, 2011, https://www.scientificamerican.com/article/tracking-cyber-hackers/.

attack, removing any doubt of who the perpetrator is. The decision to retaliate to a kinetic attack on a government or military satellite will be made on the *jus ad bellum* level based on four principles which determine what the lawful reaction may be.

Principle 1: Military Necessity. If State A decides to target a government or military satellite that is used for any function that is sovereign property of State B, that action goes against article 2(4) of the UN charter and they become belligerent for their use of force against the attacked state. It would be necessary for State B to immediately retaliate. What the counter-offensive should be will be reviewed in a separate principle. However, any of the belligerent nation's government or military resources they have in space, on the ground, or in cyber could be targetable under the premise that they are targets of a necessary military objective. If the targeted objective remains a strategic objective and places State B at an operational advantage, resources both in space and on the ground are targetable.

Principle 2: Distinction and Discrimination. A belligerent state (State A) attacking another state's (State B) government or military satellite with an ASAT missile launched from a site within its borders clearly warrants a counterattack from state B. What options does the law of armed conflict leave available for the State B to target? State B's military must discriminately target clear military objectives of the belligerent state. These options include targeting one of the State A's government or military satellites, launching a kinetic attack on State A's launch site where the initial attack originated from, or perhaps even declaring war on the State A and deploying ground troops. The ultimate decision, however, depends greatly on circumstance, and any of the choices bear great consequences that State B may not want to have be the outcome. Discrimination is important in the case of a kinetic attack in space due to the many commercial and civil satellites that are in orbit. Based on data by the UCS, of the 1,007 operational satellites that the United States has in orbit, more than 65% are either civil or commercially owned and operated.[23] Assuming that the data is similar in other countries (or according to intelligence gathered), a state must perform a surgical strike on an enemy's satellite that will have the least effect on civilian communication and navigation, knowing that there is a high number of civilian satellites in orbit.

23. "UCS Satellite Database."

Principle 3: Proportionality. When targeting another state's assets in space, it must be clear that the outcome is proportional with the attack that the belligerent actor conducted, and that little to no civilians are endangered or affected. In this scenario where state A attacked state B in a kinetic strike, state B must take into account proportionality when analyzing the situation on the jus ad bellum level in order to perform a legal counterattack that somewhat mirrors the belligerent state's attack in level of force.

Principle 4: Unnecessary Suffering. The danger of any attack or retaliation is the collateral damage that could injure or kill innocent civilian bystanders. If state B happens to destroy any of the opposing state's communication satellites, could innocent lives be threatened? Could innocent people somehow die as a result? These factors must be considered when making a decision to conduct a counter-offensive operation, be it in space or on the ground. Realistically evaluating this situation, one can infer that little to no harm will be done to civilians in the event that a civilian satellite is destroyed, although there is a small probability that emergency communication could be interrupted, putting innocent lives at risk.

Another small risk is the possibility of a destroyed satellite, either military or civilian, to reenter Earth's atmosphere and cause unprecedented damage on the ground. However, looking at past examples in ASAT operations such as the 2008 operation Burnt Frost conducted by the United States[24] and the recent event of India shooting down one of its own satellites in early 2019 show that any debris that reenters the atmosphere will burn up and that the actual major threat in destroying a satellite is the exponential threat it causes to the international space station. More than 900,000 pieces of trackable debris (larger than 10 cm) in orbit right now that pose a large risk to the ISS and other assets in space.[25] Based on this information, it can be assumed that little to no risk will involve civilians, and that real-time intelligence will assure that there is no risk involved.

24. Nicole Petrucci, "Reflections on Operation BURNT FROST," Air Power Strategy, March 6, 2017, http://www.airpowerstrategy.com/2017/03/05/burnt-frost/.

25. Michael Safi and Hannah Devlin, "'A Terrible Thing': India's Destruction of Satellite Threatens ISS, Says Nasa," *The Guardian*, April 2, 2019, https://www.theguardian.com/science/2019/apr/02/a-terrible-thing-nasa-condemns-indias-destruction-of-satellite-and-resulting-space-junk.

Scenario 2: State A Attack Against State B Civilian Satellite Used by the Military

This is much more complicated, as it will be a lot harder to determine if the attack violates the UN charter or what the proper response to this attack would be. This scenario will be also examined by the same four principles from above.

Military Necessity. Whether or not a state can conduct a kinetic attack on another state's civilian satellite depends much on what the satellite is used for. As stated above, the four main functions of a satellite are communications, ISR, missile warning, and PNT. Depending on the mission objective, any of these satellites are targetable to disrupt communications, surveillance, early warning systems, and navigation. The only two functions a civilian satellite would have are communications and/or PNT. An example of this would be if a state had a widespread commercial cell service, like Verizon or Huawei, that incidentally also ran encrypted military communication. Depending on the percentage of military traffic versus civilian traffic, and what kind of information is being transferred and its level of importance, this satellite could become targetable.

Distinction and Discrimination. There are fewer options when it comes to attacking another state's sovereign material in space. Discriminatory kinetic attacks are likely to be impossible if both government and commercial entities are using the same satellite. In this case, a non-kinetic method would be the best option to reach the objective, such as using lasers or hacking into the system remotely. The priority here is to leave civilian traffic unaffected.

Proportionality. Much like the first scenario, proportionality is a major factor in the level of potency of any counterattack. In the case that a civilian satellite that harbors military traffic must be destroyed in its entirety, close calculations must be made in order to know how much of the satellite is being used for commercial purposes (and what those purposes are), and how much of the satellite traffic is used for military or government purposes (and what those purposes are). This is necessary in order to ensure the least amount of damage done to civilian infrastructure. If sufficient intelligence proves that an attack would be appropriately proportionate, then it may be targetable.

Unnecessary Suffering. The results of this scenario would mirror those of the previous scenario. Even though life-threatening risk to

civilians is very unlikely, states must be responsible and ensure that all risk to civilians is mitigated.

Non-Kinetic Threats

There are more ways than one to infiltrate another state's assets in space; explosive and violent means are no longer the first choice when conducting such an operation. The more attractive options to quietly and perhaps clandestinely disengage an enemy satellite are the non-kinetic means. This includes high-power microwaves, radio frequency jammers, signal jammers, and lasers. These methods are known as direct energy weapons (DEW) and the effects can last anywhere from a short period up to and including permanently damaging the target.[26] These methods can be used in a much more effective way to mitigate risk to civilian communication lines or navigation. In order to conduct an entirely discriminatory operation, however, one of the most effective methods of infiltration is through the cyber domain. Cyberattacks in space are one of today's leading threats as assets in space are vulnerable to being hacked. It is very difficult to trace the perpetrators making this an attractive option for belligerent states to use. Discrimination is important in the event of a cyberattack from a belligerent state as it is very important to be sure of the source of the attack before retaliating. Proportionality is also a major issue. For example, if State A hacks State B's military satellite and compromises encrypted communication, this does not necessarily permit State B to declare war and invade State A. However, perhaps State B can destroy or disrupt one of State A's satellites, or maybe State B can disrupt or destroy ground assets that are facilitating the cyberattacks.

There are many threats that are presenting themselves in the space domain which threaten the United States as more states grow and develop their own capabilities. It is imperative that the United States devotes ample time and resources to the development of weapons and defenses in space in order to maintain global superiority. This must be done with the same level of urgency of the original space race and rush to develop the atomic bomb during the Cold War. Notwithstanding, as with the development of the atomic bomb, great care and caution should be taken as the legal parameters are set and solidified regarding the use of kinetic and non-kinetic weapons and methods in space.

26. *Challenges to Security in Space*, 9.

Warfare in space should be ethical and should not undermine humanity where it can be controlled. With the creation of the Space Force, the United States is on the right track as it focuses more on the final frontier and prepares for a battlefield that was unprecedented not too long ago.

Contributors

Cash Holdaway is a junior studying National Security at Utah Valley University. Growing up in a military family, he has always felt the need to serve his country and community and hopes to continue to do so after earning his degree. Aside from his studies, Cash serves part-time with the Utah National Guard, where he fulfills his role supporting combat operations through intelligence collection. Upon graduation, Cash hopes to have a fulfilling career in the National Security Enterprise as well as continuing his military service.

Joshua Jones is currently a senior at Utah Valley University. He is pursuing his bachelor's degree in Legal Studies with a minor in National Security studies. Currently, he works as a legislative assistant to Rep. Val Peterson of District 59 at the Utah state Capitol for the 2020 Legislative session. Joshua also works for Atlantic Key Energy in Florida selling solar. He plans to attend law school upon graduation from UVU and on pursuing a career as an attorney in civil service or in the national security field. His hobbies include exercising any chance he gets to, going to the gym, going out with friends and family and being social.

Alyson Hatch is a junior at UVU studying communications, national security, and Russian. She has a strong interest in cyber warfare and intelligence. Recently she was a part of UVU's first team to participate in the Atlantic Council's Cyber 912 competition. She has previously served as the social media administrator for the National Security society. This past semester she took a break from her studies to work and travel but plans to return to UVU in the fall.

Bryce Krieger is a senior at Utah Valley University, anticipating graduation in May of 2021 with a Bachelor of Science in National Security

Studies. He intends to continue his education beyond UVU with a J.D. and hopes to attend law school in the Washington DC area. In the long term, he desires to utilize his education to pursue a career in public service, providing legal counsel to the federal government. Bryce transferred to UVU in 2018 determined to finish his degree and maximize his undergraduate experience by engaging on campus. Through his involvement with the Center for National Security Studies he participated in the 2019 summer seminar in Washington DC and also joined UVU's first team to compete in the Atlantic Council Cyber 9/12 Strategy Challenge. Currently, Bryce is a Presidential Intern at UVU assigned to the Office of General Counsel. Bryce is supported by his wife, Danica, and his son, with whom he shares a name.

Arik Bryton Nelson is from American Fork, Utah. He is currently majoring in NSS and minoring in Languages and Political Science. Bryton is a cadet with the Air Force and plan to commission and serve in the armed forces after he graduates. He loves to cook, read, and spend time with his wife and friends.

Brandon Amacher is a senior at Utah Valley University. He is pursuing a degree in integrated studies with emphases in business management and national security studies. Brandon is fluent in Spanish and is on track to earn the highest recognition offered to foreign students by the government of Spain and the University of Alcalá for business Spanish. Brandon was born in Sandy, Utah, to a Cuban-American family and was raised to honor and protect American values. He currently works in government relations and marketing at a cybersecurity firm. Following college, Brandon hopes to peruse graduate degrees in business administration and public policy and to start a family with his wife, Aulola.