DETERRENCE THROUGH ENTANGLEMENT

A Dissertation
Presented to
The Academic Faculty

by

Brian C. Stewart

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
Sam Nunn School of International Affairs

Georgia Institute of Technology
August 2022

DETERRENCE THROUGH ENTANGLEMENT

Approved by:

Dr. Mariel Borowitz, Advisor
School of International Affairs
Georgia Institute of Technology

Dr. Rachel Whitlark
School of International Affairs
Georgia Institute of Technology

Dr. Jenna Jordan
School of International Affairs
Georgia Institute of Technology

Dr. Erik Lin-Greenberg
Department of Political Science
Massachusetts Institute of Technology

Dr. Maggie Kosal
School of International Affairs
Georgia Institute of Technology

Date Approved: June 27, 2022

To Levi, Millie, Mom, Dad, and Anna

ACKNOWLEDGEMENTS

I would like to thank my advisor and committee members for shepherding me through this incredibly challenging and humbling journey. I would also like to thank the other faculty members at Georgia Tech who have expanded my thinking along the way. Most importantly, I would like to thank my family for their unending support in what proved to be one of the most difficult periods of my life. To my children, Levi and Millie, who have endured so many hard goodbyes, multiple cross-country moves, and who adjusted to life during a pandemic with bravery and courage, I'm so proud and thankful to be your dad. To my parents, thank you for supporting me and helping me, at all times, no matter what crazy ideas I decide to pursue in life. To Anna, thank you for believing in me, caring for me, and giving me hope; you sustain me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

ABM	Anti-ballistic Missile
ASAT	Anti-satellite
C2	Command and Control
CSIS	Center for Strategic and International Studies
DoD	Department of Defense
DV	Dependent Variable
EMP	Electromagnetic Pulse
GAO	Government Accountability Office
GPS	Global Position System
I&W	Indications and Warnings
IC	Intelligence Community
IR	International Relations
ISR	Intelligence, Surveillance, and Reconnaissance
IV	Independent Variable
KP	Kinetic Permanent
LEO	Low-Earth Orbit
NATO	North Atlantic Treaty Organization
NC3	Nuclear Command, Control, and Communication
NL	Non-kinetic, Localized
NP	Non-kinetic Permanent
NR	Non-kinetic Reversible
NSC	National Security Council

NTM	National Technical Means
NUDET	Nuclear Detonation
PNT	Position, Navigation, and Timing
RAAF	Royal Australian Air Force
RAND	Research and Development
RPO	Rendezvous and Proximity Operations
SALT I	Strategic Arms Limitation Treaty 1
SATCOM	Satellite Communications
SDA	Space Domain Awareness
SDI	Strategic Defense Initiative
SSA	Space Situational Awareness
START	Strategic Arms Reduction Treaty
SWF	Secure World Foundation
T	Teams
U.S.	United States
UK	United Kingdom
USA	United States Army
USAF	United States Air Force
USSF	United States Space Force
USSPACECOM	United States Space Command

SUMMARY

Many components of the Nuclear Command, Control, and Communications (NC3) architecture of the United States are vulnerable space systems. These space systems, which include intelligence, surveillance, and reconnaissance (ISR), missile warning, and satellite communications (SATCOM) systems, are considered entangled, which means they support both strategic (nuclear) functions as well as tactical (conventional) missions. Space security experts believe these entangled NC3 systems could be attractive targets for adversaries, even in low-level regional or conventional conflicts, due to the U.S. military's heavy reliance on these capabilities to project power and observe adversary activity. Some scholars claim that the entangled nature of these systems combined with the apparent willingness of adversaries to attack these systems crates a significant risk of inadvertent escalation. In their view, a state could be forced to escalate a conflict beyond what either party intended due to the strategic-level impacts that could occur as a result of attacks against NC3 systems.

In order to mitigate these risks, the U.S. government has adopted a strategy of disentanglement and tens of millions of dollars have been spent to begin the process of disentangling systems. Unfortunately, the Department of Defense (DoD) has not thoroughly studied the potential effects of disentanglement on stability, security, and deterrence. The Government Accountability Office (GAO) wrote a report in 2015 questioning whether this strategy would actually reduce the risks of inadvertent escalation and cautioned against possible second and third-order effects, namely a weakening of deterrence. Additionally, recent research calls into question the logic of

inadvertent escalation. The U.S. Government is spending millions of dollars on a problem that is not well understood, and these actions could actually make space systems less safe.

I challenge the logic of disentanglement and offer a theory of deterrence through entanglement. I argue that potential adversaries understand that attacks against entangled NC3 systems affect both nuclear and conventional missions and as such, expect that attacks against these vital national assets could be met with the harshest possible response, up to and including nuclear retaliation. With entangled space systems, a potential adversary must be willing to accept strategic consequences even if they only seek tactical objectives, so the cost-benefit calculus for decision makers should ultimately favor deterrence. Continuing this logic, I argue that disentangling NC3 systems could make conventional versions of the systems less dangerous targets and therefore more susceptible to attack. By lowering the expected costs and expected severity of retaliation for attacks, an adversary could be more willing to target disentangled NC3 space systems.

I test my theory with novel experimental wargaming scenarios and an elite sample survey that feature entanglement as the independent variable (IV) and operationalize deterrence as a dependent variable (DV), as measured through attacks against space systems. I also conducted a public opinion survey to gauge perceptions about space system attacks again using entanglement as the IV. The wargaming sessions were conducted with undergraduate and graduate students at the Georgia Institute of Technology and provide strong support to my theory of deterrence through entanglement. The wargaming sessions demonstrated that entanglement deterred attacks against space systems better than disentanglement, with entangled systems a third as likely to be attacked as disentangled systems. Not only were entangled systems less likely to be

attacked, when they were attacked, attacks were less severe than with disentangled systems. Based on both quantitative and qualitative data, entangled systems often carried too high a risk of escalation to justify attacks whereas disentangled systems were viewed as safer options and were attacked more frequently and with more severe methods. Entanglement also appeared to deter attacks in general; out of 20 teams that did not conduct any attacks during the wargaming sessions, 18 were from the entangled treatment.

The elite surveys sampled military members in the space community and while these surveys did not demonstrate that entanglement affected the decision to attack NC3 space systems as a whole, entanglement did appear to deter attacks against missile warning systems, and respondents in the entangled treatment were three times more likely to cite fear of escalation as the primary factor for not attacking space systems. The elite surveys also showed interesting differences in perceptions of severity based on whether a respondent was the attacker or victim. On a 1 through 9 scale of response severity, scores were a full point higher on average if the respondent was the victim compared to the attacker, for the same type of attack. Finally, the public surveys did not show significant differences between entanglement treatments and recommended response, though there were significant differences in perceptions of kinetic vs. non-kinetic attacks. Respondents in the entangled treatment did support more severe responses, on average, and were less likely to support soft power measures, however the biggest factor affecting response decisions was proportionality.

In both the wargames and surveys, disentangled nuclear systems were least likely to be attacked of all. These systems are unambiguously strategic in nature and as a result

participants were more hesitant to conduct attacks against these systems in support of conventional objectives, though attacks did occur. Moving forward, policy makers would need to weigh priorities with respect to space system attacks. If the goal is to minimize the number of attacks against nuclear systems above all else and accept that conventional systems might be more likely to be attacked, disentanglement could still prove to be a useful strategy. However, if the goal is to deter the greatest number of attacks overall, entanglement should probably be preserved. Additionally, with a relatively small sample size for the elite survey, findings failed to yield statistical significance. Despite these issues, this research succeeds in arming the academic and broader communities with the first-ever empirical data to support discussions and investigations on entanglement.

Some other interesting findings emerged from the research, including an aversion to kinetic weapons and acceptance of cyber weapons. Cyber weapons were generally regarded as safe and effective options for attacks by participants across all treatments. If the data are any indication of future events, cyber weapons will likely play a significant role in conflict moving forward. Additionally, my research revealed interesting findings with respect to human psychology. The disparity in perceptions of severity for respondents based on whether they were the victim or attacker finds support in behavioral economics and could be a source of misperception for leaders assessing likely responses to their actions. The effects of human psychology were also on display in a wargaming session conducted on the heels of Russia's invasion of Ukraine. Participants in this session accounted for just 14% of total participants but conducted over 50% of all non-space related military attacks. Additionally, 6 of the 12 teams involved conducted

conventional ground assaults, compared to just 1 of the other 72 teams from other sessions. This supports the notion that external factors can bias experimental

My research contributes to space security and entanglement scholarship in a number of ways. Most importantly, this is the first-ever empirical analysis of space system entanglement. While scholars have conducted space security wargames, elite and public surveys, and other types of space security analyses in the past, none have used entanglement as a variable. More broadly, my research further demonstrates the possibility and utility in experimental approaches to space security studies. Importantly, through my research I have challenged widely held beliefs that disentanglement contributes to deterrence and demonstrated that not only are disentangled systems more likely to be attacked in future conflicts, but they will also likely face more severe attacks than entangled systems due to the perceived lower risk of escalation. This finding alone should give pause to leaders advocating for increased disentanglement in the U.S.' NC3 architecture. I also challenge the notion that disentangled nuclear systems will be viewed as "clearly off limits," as these systems were attacked in both the wargames and elite surveys. If this assumption is being used to inform policies and strategies within the U.S. government, my research shows that this could be a dangerous misperception. Overall, my research provides new data with which to assess entanglement and perceptions about space conflict, both from elite populations and the public. These data can be used to inform better policies and strategies for space moving forward.

CHAPTER 1. INTRODUCTION

"There is something more important than any ultimate weapon. That is the ultimate position - the position of total control over Earth that lies somewhere out in space. That is the distant future, though not so distant as we may have thought. Whoever gains that ultimate position gains control, total control, over the Earth, for the purposes of tyranny or for the service of freedom."
— Lyndon B. Johnson, United States Senator, 1958[1]

Space security challenges and competition in space are not new. The quote above shows that leaders in the United States (U.S.) Government were concerned and talking about space security within a year of Sputnik's launch and space weapon development began in earnest around the same time these remarks were made. Fortunately, peace has largely prevailed in space; no kinetic space weapons have been used in anger, though many have been tested. However, there is a growing consensus that future wars will be at least partially fought in the space domain, and some claim that attacks against space systems are inevitable.[2] Space has become more congested, contested, and competitive than ever before as access to space has expanded far beyond the global superpowers, and weapons that can be used to target space systems continue to be developed, tested, and proliferated.[3] Even still, warfare in space is not a foregone conclusion, and actions can be taken to preserve and strengthen deterrence.

Despite its importance, space security has received limited attention among International Relations (IR) and security scholars relative to other issues, and many of the IR concepts that have been applied to the space domain have not been rigorously scrutinized or empirically tested. I focus specifically on the prevailing belief in the

[1] Westenhoff, C. M. (2007).
[2] AFSPC (2016), 9; Moltz, J. C. (2008), 25; Harrison, T., Cooper, Z., Johnson, K., & Roberts, T. G. (2017), 8-9.
[3] Harrison, T., Johnson, K., Moye, J. and Young, M. (2021); Secure World Foundation (2021); National Space Society (2021); Gohd, C. (2021).

academic community as well as in the Department of Defense (DoD) that Nuclear Command, Control, and Communications (NC3) space systems are likely to be attacked in future conflicts, and that the entangled nature of these systems creates a very significant risk of inadvertent escalation.[4] As a result of this assumption, the DoD has invested tens of millions of dollars to disentangle NC3 space systems.[5] There are a number of important problems with this line of reasoning, however. First, inadvertent escalation as a result of entanglement has neither been observed in the real world nor empirically tested, and some scholars suggest the problem is both overstated and unlikely.[6] Second, the possible deterrence value of entanglement has not been tested. Third, the effects of disentanglement on adversary perceptions have not been addressed. Finally, real-world acquisition decisions are being made based on these assumptions and the window for assessing alternative policy options is rapidly closing. Through my research, I provide the first empirical evidence to assess assumptions about disentanglement as a strategy for space security. I present a theory of deterrence through entanglement that increases the body of knowledge in the space security arena and can be used by policy makers and strategists to inform future national security space system design and acquisitions.

My theory of deterrence through entanglement is centered upon expected consequences for attacks against NC3 space systems. Deterrence is "persuading an opponent not to initiate a specific action because the perceived benefits do not justify the

[4] Entanglement refers to the dual nuclear-conventional nature of NC3 space systems. The term will be defined further in subsequent sections.
[5] Erwin, S. (2021); Government Accountability Office (2019), 3-4.
[6] Kroenig, M. and Massa, M. (2021).

estimated costs and risks."[7] When a state's nuclear capabilities are at stake, threats of punishment are more credible, and expected costs and risks are at their highest. According to current U.S. policy, the employment of nuclear weapons could be considered in response to non-nuclear strategic attacks, to include attacks on "command and control, or warning and attack assessment capabilities."[8] While some might argue that it is unlikely the U.S. would use nuclear weapons in response to attacks against satellites, it is the "threat that leaves something to chance" and the possibility of uncontrolled escalation to nuclear war that provides such a strong deterrent to would-be attackers.[9] Of course, it is this potential for unrestrained escalation that proponents of disentanglement also cling to, and ultimately the argument I lay out harkens back to a classic competition in risk taking. Does disentanglement weaken deterrence? How do adversaries perceive attacks against entangled and disentangled space systems? These questions have major implications in the real world, yet they've never been addressed empirically. All that exists now are speculation and assumptions. This gap in research is where I step in.

I argue that potential adversaries understand that attacks against entangled NC3 systems affect both nuclear and conventional missions and as such, expect that attacks against these vital national assets could be met with the harshest possible response, up to and including nuclear retaliation. As a result, only the most brazen and determined adversary should be willing to accept the risks of attacking entangled space systems. With entangled space systems, an adversary must be willing to accept strategic

[7] Mearsheimer, J. J. (1985), 14.
[8] Office of the Secretary of Defense. (2018). Nuclear Posture Review. Washington D.C.: Office of the Secretary of Defense, 21.
[9] Schelling, T. (1980).

consequences even if they only seek tactical objectives, so the cost-benefit calculus for decision makers should ultimately favor deterrence. Continuing this logic, I argue that disentangling NC3 systems could make conventional versions of the systems less dangerous targets and therefore more susceptible to attack. By lowering the expected costs and expected severity of retaliation for attacks, an adversary could be much more willing to target disentangled NC3 space systems.

I test my theory with novel experimental wargaming scenarios and an elite sample survey that feature entanglement as the independent variable (IV) and operationalize deterrence as a dependent variable (DV), as measured through attacks against space systems. I also conducted a public opinion survey to gauge perceptions about space system attacks again using entanglement as the IV. The wargaming scenarios were conducted with undergraduate and graduate students at the Georgia Institute of Technology and demonstrated that entanglement deterred attacks against space systems better than disentanglement, with entangled systems a third as likely to be attacked as disentangled systems. Not only were entangled systems less likely to be attacked, when they were attacked, attacks were less severe than with disentangled systems. The elite surveys sampled military members in the space community and while these surveys did not demonstrate that entanglement affected the decision to attack NC3 space systems as a whole, entanglement did appear to deter attacks against missile warning systems. The surveys also showed interesting differences in perceptions of severity based on whether a respondent was the attacker or victim. Finally, the public surveys did not show significant differences between entanglement treatments on severity of response, though there were significant differences in perceptions of kinetic vs. non-kinetic attacks.

In this chapter, I will first introduce key terms related to this research and identify the space systems my theory covers, as well as define entanglement. Following that, I provide background on competition in space historically and how it has evolved. I also apply IR concepts to the space domain to help explain the volatility in space today and identify threats to space systems to justify why these issues are so important. With the importance of this topic established, I then move on to frame the discussion about entanglement. Finally, to conclude the chapter I discuss the relevance of this research and present a summary of my findings.

1.1 Key Terms

1.1.1 NC3 Space Systems

The particular set of space systems that I focus on in my research are NC3 space systems. From the beginning of space operations, governments have relied on space systems for critical strategic functions like treaty verification, missile warning and defense, strategic communication, and command and control (C2). The United States heavily integrates space into its NC3 architecture and the primary space systems that are included are: space-based missile warning satellites, protected satellite communications (SATCOM) satellites, and national technical means (NTM) intelligence, surveillance, and reconnaissance (ISR) satellites, along with the accompanying C2 nodes, communications links, and other supporting infrastructure.

Missile warning satellites provide early warning of launches around the world, before RADAR or other means might detect a launch. This early warning is critical not only for initiating a response, but for missile defense as well. Protected SATCOM satellites enable the President and senior decision makers to send and receive critical

information, even in degraded environments. These systems would be used to issue nuclear launch orders, should the need arise. NTM ISR systems are used not only for treaty verification and compliance monitoring, but also to provide valuable intelligence on the actions of others, including indications and warnings (I&W) of impending launches. In addition to the strategic functions mentioned above, these same satellites support tactical and conventional missions as well. For example, strategic missile warning satellites are also used to provide theater warning and battlespace awareness information to tactical users. Protected SATCOM systems and NTM ISR satellites also support tactical missions. This dual-function, strategic-conventional nature of NC3 systems is referred to as entanglement, which I further define in the next section.[10]

1.1.2 Entanglement

For the purposes of my research, entangled systems are those systems that perform both nuclear and conventional missions.[11] Specifically, I include entangled missile warning, protected SATCOM, and NTM ISR space systems. I use the term "entangled" to refer to these systems because that is the term that is most commonly used in existing literature, although some literature uses the terms "dual-use" or "aggregated" to refer to the same conditions. One of the challenges in studying space system entanglement is the lack of consistency with terms, so I will briefly differentiate between entangled, aggregated, and dual-use systems below.

[10] The specific characteristics, capabilities, and numbers of U.S. NC3 space systems are classified, but these details are not necessary to understand the strategic importance of these systems, nor are they necessary to test perceptions about entanglement, which I accomplish using notional capabilities in my empirical chapters.

[11] Other types of space system entanglement will be discussed in Chapter 2.

The NC3 systems mentioned above are considered entangled because they perform both nuclear and conventional missions simultaneously and utilize the same sensors, processing, data links, etc. For example, the sensors on U.S. missile warning satellites are used to detect strategic/nuclear missile launches as well as to detect conventional/tactical missile launches and the data are downlinked together and processed together. NTM ISR satellites can be used to verify nuclear missile sites (strategic/nuclear) or collect intelligence on terrorist encampments (conventional/tactical) and this data can be collected on the same imaging pass and downlinked at the same time; the missions and capabilities are completely integrated.[12] Similarly, the antennas and transponders on protected SATCOM systems could be used to send nuclear launch codes from the President (strategic/nuclear), or to support a video teleconference between battleships (conventional/tactical) simultaneously. All of these systems are therefore considered entangled.

Despite the use of entanglement throughout academic literature, the DoD uses the term aggregation to refer to the NC3 space systems I am investigating; but these terms should not be used synonymously. The DoD does not provide a definition for aggregation but instead says that "disaggregation is defined as the separation of dissimilar capabilities into separate platforms or payloads."[13] The dissimilar capabilities referred to include not only the entangled strategic/nuclear and conventional/tactical capabilities referenced above, but also capabilities on non-NC3 systems that exist as a result of hosted payloads or multi-mission satellites. The problem with using the term aggregation instead of

[12] A "pass" refers to the satellite flying over (or passing by) target areas. Multiple collections can occur on each pass.
[13] Office of the Assistant Secretary of Defense for Homeland Defense and Global Security (2015), 6. Joint Chiefs of Staff. (2020), I-9.

entanglement is a matter of specificity. Disaggregated systems could still be entangled, and aggregated systems could be disentangled.

I define aggregated space systems as systems that feature an array of different sensors, missions, and/or capabilities onboard a single spacecraft without those functions being co-dependent. For example, the nuclear detonation detection (NUDET) capability on global positioning system (GPS) satellites is not integral to the primary mission or signals that provide position, navigation, and timing (PNT). Vice-versa, the PNT antennas onboard the satellite could be jammed or turned off without affecting the NUDET capability. Therefore, NUDET is an aggregated capability, it is not entangled. Other examples of aggregated capabilities include hosted payloads, where the primary mission of the satellite is distinct from the mission of the additional payload. While these missions may share spacecraft resources, like fuel and power, they operate independently of each other. Conversely, entangled systems utilize the same sensors, links, processing and command and control simultaneously. As a result, *attacks against entangled systems inherently affect all missions*. An adversary cannot disable only the theater warning capability of a missile warning sensor, or only the tactical communications of protected SATCOM systems, or only the tactical imaging capabilities of NTM ISR satellites. An aggregated capability could be attacked independently of other missions onboard that spacecraft (assuming the spacecraft itself was not the target). While the DoD bundles everything under the umbrella of aggregation, the different characteristics of entangled versus aggregated systems mentioned above warrant specific terminology and that is why I use the term entanglement in my research. When the DoD refers to NC3 systems as aggregated, the more correct term would be entangled.

"Dual-use" is also sometimes used to refer to entangled systems, and has a number of different meanings, but the United States Government generally uses the term to refer to systems that have both military and civilian applications.[14] This is what most people think about when they encounter the term dual-use, however the term can also be used to refer to systems that are capable of both peaceful and hostile actions, as well as systems that have both nuclear and conventional missions. Dual-use is not an incorrect term per se, but I use the term entangled for specificity, clarity, and consistency with existing literature.

1.2 The Space Environment Yesterday and Today

1.2.1 How We Got Here: A Brief History of Orbital Warfare

The United States and Soviet Union began developing and testing anti-satellite (ASAT) weapons during the early days of the space age and continue to develop both offensive and defensive space weapons today. In the last couple of decades, emerging space powers like China and India have also developed and tested their own ASAT capabilities. While there has never been a hostile employment of a kinetic space weapon, these systems have played an important role in both diplomacy as well as military strategy for the last 70 years. As satellites have grown in importance and capability, particularly those that support military operations and strategic defense, weapons to degrade or destroy these capabilities evolved, often faster than policy could match. Today, there is still no coherent policy to define what a space weapon is, let alone enforce any restrictions on development or deployment, and the number of actors who possess these capabilities continues to grow.

[14] U.S. Department of Commerce. (2020).

The Soviet Union began a co-orbital ASAT program in 1963 and conducted seven close approaches over subsequent years before declaring their system operational in 1973. Throughout the 1970s, the Soviet Union continued to develop and test co-orbital ASATs with four tests in both 1976 and 1977 and one test a year from 1978-1982.[15] The United States did not have any purposefully designed co-orbital ASATs or direct-ascent ASATs in development or testing early in this period, which was a matter of debate within the U.S. government. This issue came to a head in 1976 when a space panel under the National Security Council (NSC) issued a classified report to the President concerning ASAT development. The panel stated, "there is an urgent need for the U.S. to have the capability to destroy a few militarily important Soviet space systems in crisis situations or war."[16] This determination was based on the belief that the Soviet Union possessed an asymmetric advantage over the U.S. with their capabilities to destroy vital U.S. satellites, and the prescient prediction that "real-time space capabilities will become even more important to the effective use of military forces in the future."[17]

Despite this belief, there were significant policy considerations that affected the U.S.' early ASAT programs. The first Strategic Arms Limitation Treaty (SALT I) signed in 1972 and the Anti-Ballistic Missile (ABM) Treaty that followed shortly thereafter prohibited interfering with or attacking space systems used for verification and monitoring, and the Soviet Union enacted a self-imposed moratorium on ASAT testing for a brief time during this period.[18] Additionally, there was disagreement between the intelligence community (IC) and DoD on the net effect of ASATs, with some IC

[15] Grego, L. (2012), 3-5.
[16] Smith, R. (1976), 1.
[17] Smith, R. (1976), 1.
[18] Stares, P. (1985), 134; Siddiqi, A. (1997), 233; Bateman, A. (2022), 5.

members believing that ASATs would lead to increased hostility in space and threaten the critical ISR systems that were vital not only to treaty verification, but to all of the other missions supported by photo reconnaissance.[19] This debate finds some renewed ground in the research I am undertaking, and whether strategies designed to increase security could ultimately lead to greater insecurity. Finally, an overarching concern expressed by former National Security Advisor Brent Scowcroft was that "the lack of a clearly articulated statement of national security policy relative to the use of space has delayed U.S. development of available countermeasures for years and has contributed to our current vulnerable posture in space."[20] Nevertheless, the U.S. accelerated previously underway efforts to field a limited ASAT capability to target low-Earth orbit (LEO) Soviet spacecraft, including the very systems protected by existing treaties.

When President Cater took office, he prioritized strengthening treaties and pursuing diplomacy in space and he viewed ASATs as potentially harmful to that end. As a result, he ordered a pause on ASAT development, a review of existing programs, and ultimately issued a policy that sought to ban kinetic space weapons, though he supported the continuation of "some R&D…as a hedge against Soviet breakout."[21] Both the Soviet Union and U.S. continued work on ASAT programs in the 1970's while simultaneously pursuing further treaties to strengthen nuclear stability; but, changes in administrations in both states brought further changes to the respective space programs. In the mid-1980s, the United States developed and tested air-launched ASATs with the Celestial Eagle program, and one test in 1985 destroyed a U.S. satellite and generated thousands of

[19] Smith, R. (1976), 6.
[20] Scowcroft, B. (1976), 1.
[21] Brzezinski, Z. (1977); Bateman, A. (2022), 11-13.

pieces of debris. This testing was on the heels of a second Soviet moratorium on ASAT testing in 1983 and both factors led the U.S. to ban ASAT testing in 1986 and cancel the Air Force's ASAT program in 1987. In 1987, the Soviet Union tested a space battle station, which President Gorbachev was supposedly unaware of, and once he became aware, he cancelled future funding for the program.[22]

These program cancellations and moratoriums led to a brief but quiet period in space weapon development and testing for the world. In 1989, the Soviet Union allowed a U.S. delegation to inspect a laser that could be used to target satellites to demonstrate that it was not powerful or accurate enough for destruction, and as a result the U.S. Congress banned testing of lasers from 1991-1995. However, the Air Force used a laser to blind a satellite in 1997, which was viewed by Russia as a violation of the ABM treaty. During this period, the U.S. Army also tried to enter the ASAT arena and Congress earmarked funding for their program in 1996, but it was vetoed by President Clinton. This program was also opposed by the Air Force who viewed kinetic ASATs as too dangerous because of debris creation, which had become a more pressing concern due to the increased use of space both militarily and commercially. The Army program continued to survive until Senator Robert Smith of New Hampshire, the program's primary advocate, was not re-elected in 2002.[23]

The re-arming of space, or at least more focus on weaponization reignited when George W. Bush was elected president in 2000.[24] In the early 2000s, both the Air Force and NASA developed rendezvous, and proximity operations (RPO) spacecraft that could

[22] Grego, L. (2012), 3-5.
[23] Grego, L. (2012), 4-8.
[24] Moltz, J. C. (2008), 11-13.

be perceived as threatening, even though the ability to perform RPO had been demonstrated in the early days of human spaceflight. The United States also withdrew from the ABM Treaty which allowed for development of new space capabilities.[25] The situation became more complicated when China tested an ASAT in 2007 that created thousands of pieces of debris and served as a wake-up call for many inside and outside of the space community.[26] This test demonstrated the emergence of new players into space competition, which had previously been dominated by the U.S. and Russia and signified the end of the perceived peace that existed in space since the U.S. and Soviet Union agreed to end ASAT testing in 1985.[27]

In 2008, the U.S. Navy used a standard missile 3 (SM-3) to shoot down a malfunctioning national security spacecraft in order to limit risks to people and structures on Earth. However, this event was viewed by many as a direct response to the Chinese test.[28] Regardless of intent, the event demonstrated to the world that the U.S. still maintained the capability to shoot down satellites, and in this case using a system that was never designed for this purpose explicitly. This speaks to the challenges of defining space weapons, as systems not expressly designed for that purpose can be effectively utilized to destroy spacecraft.

---

[25] Moltz, J. C. (2008), 307-308.
[26] Weeden, B. (2010). 2007 Anti-Satellite Test Fact Sheet. Washington, D.C.: Secure World Foundation.
[27] Harrison, T., Cooper, Z., Johnson, K., & Roberts, T. G. (2017). Escalation and Deterrence in the Second Space Age. Washington, DC: Center for Strategic and International Studies, 2.; Grego, L. (2012, January). A History of Anti-Satellite Programs. Retrieved from Union of Concerned Scientists: https://www.ucsusa.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf, 5.
[28] Grego, L. (2012, January). A History of Anti-Satellite Programs. Retrieved from Union of Concerned Scientists: https://www.ucsusa.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf, 12.; Department of Defense. (2008, February 21). DoD News Briefing with Gen Cartwright from the Pentagon. Retrieved from Department of Defense Press Operations: https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=4152

In subsequent years, the U.S., China, and Russia have continued to develop and test systems that could be used as weapons, though few have been expressly labeled as such, particularly kinetic weapons. For example, China demonstrated robotics technology with the stated purpose of debris removal or on-orbit servicing of satellites, but the technology could easily be used to destroy satellites as well.[29] India has also now entered the kinetic ASAT arena with their 2020 ASAT test that destroyed a microsatellite.[30] Even after the outcry over debris-creating events, Russia has continued to test kinetic ASATs, including a test in November 2021 that destroyed a satellite and created over 1,500 new trackable pieces of debris.[31] Most recently, the U.S. has once again enacted a moratorium on ASAT testing, this time a self-imposed ban on destructive kinetic tests, and have asked others in the international community to join.[32]

Ultimately, the history of space weapons programs offers several important lessons that inform this research. From a broad perspective, this history shows that political factors are as important to space weapons development and employment as technological factors, and that military utility can be superseded by bureaucratic or other domestic considerations. More importantly though are how these developments were viewed within and without government. Prior to the 1976 space panel, many analysts believed that "the Soviet Union would not interfere with American satellites short of full-scale conflict" and that existing treaties provided "an added layer of protection."[33] However, that thinking evolved and the idea that NC3 systems could be attacked, even in

[29] Harrison, T., Johnson, K., & Roberts, T. G. (2019, 13.
[30] Weeden, B., & Samson, V. (2019).
[31] Nivedita, R. (2021).
[32] Harris, K. (2022).
[33] Bateman, A. (2022), 7.

lower-level conflict, became more widely accepted. The logic was that "non-interference provisions in arms control treaties did not extend to satellites that were used to support non-treaty verification activities" and "because intelligence satellites used for arms control verification were also being employed for tactical-military support, they would become legitimate military targets in wartime."[34]

Though many decades old now, this is a foundational logic for this research. The New Strategic Arms Reduction Treaty (New START) maintains protections for critical NC3 space systems that are required for verification, monitoring, and warning, but these entangled systems are also used to support tactical operations and are therefore considered legitimate military targets. This is the logic that leads analysts today to believe that the U.S.' entangled missile warning, SATCOM, and ISR systems are likely targets in future conflicts with peer adversaries. That said, the possible dire consequences of such attacks have also been widely discussed since the inception of ASAT programs. The 1976 space panel recommended a hierarchy "in which attacks on early-warning and nuclear command and control satellites, for example, would have more dangerous repercussions than interference with satellites not directly tied to nuclear stability."[35] In 1978, the U.K.'s ambassador to NATO cautioned that attacking these systems could lead either the U.S. or Soviet Union "to have to contemplate the first use of nuclear weapons for fear of themselves becoming the victim of a first pre-emptive strike."[36] Recognition of these facts should contribute to deterrence.

[34] Bateman, A. (2022), 7.
[35] Bateman, A. (2022), 7.
[36] Bateman, A. (2022), 12.

1.2.2 Orbital Security Dilemma, Offense-Defense Balance, and First-Strike Incentive

Security dilemmas are rooted in game theory, particularly the stag hunt, which shows that "unless each person thinks that the others will cooperate, he himself will not."[37] This fear of defection causes states to pursue security strategies that make themselves feel more secure but as a result make other states feel less secure, and therefore prone to bolster their own security. The security dilemma is evident in space with the intensely competitive environment, development and testing of space weapons, and attempts to gain and maintain "space superiority."[38] Additionally, the disentanglement strategy of the United States that I am investigating also contributes to and is influenced by the orbital security dilemma. Disentanglement is intended to preserve capabilities and deter attacks, yet preparing to fight through attacks could signal to others that the U.S. is actively preparing for space war; and these preparations for conflict could become a self-fulfilling prophecy.

The orbital security dilemma could be particularly dangerous due to perceptions that space is an offense dominant domain.[39] The implications of offense dominance have long been studied in IR literature, and generally point to greater instability, arms racing, and greater incentive for first-strike or preventive war.[40] Offense-defense balance theory claims that "when defense has the advantage over offense, major war can be avoided."[41] As offense becomes more dominant or advantageous "the security dilemma becomes

---

[37] Jervis, R. (1978), 168.
[38] Johnson-Freese, J. (2017); Moltz, J. (2008, 2012 and 2014); Townsend, B. (2020); Zhang, B. (2011).
[39] It is considered easier and cheaper to destroy space systems than defend them, hence the perception of offense-dominance. For more analysis on offense-defense balance in the space domain, see: Finch, J. and Steene, S. (2011), 11; Harrison, R., Jackson, D., and Shackleford, C. (2009), 6; Manzo, V. (2011), 3; Morgan, F. (2010)
[40] Glaser, C. and Kaufman, C. (1998), 2.
[41] Glaser, C. and Kaufman, C. (1998), 1; Lynn-Jones, S. (1995), 660-691.

more severe, arms races become more intense, and war becomes more likely."[42] The dual-use nature of many space systems makes calculations of the offense-defense balance in space extremely challenging. U.S. Army Lieutenant Colonel Brad Townsend argues that offense may have the advantage in space at the level of the individual satellite, but when looking at the aggregate space capabilities of a state, defense has the advantage.[43] Despite his belief, he recognizes that space is perceived to be an offense-dominant domain and that "this misperception of offense dominance is ruling out viable reassurance strategies and forcing states to pursue self-defeating policies that are only intensifying the security dilemma in space."[44]

Also raising the likelihood of conflict in space are perceptions of a first-strike incentive. According to Schelling, states often choose preventive war in response to fears of surprise attacks.[45] Otto von Bismarck referred to preventive war as "committing suicide from fear of death." However, Bismarck went on to say that "no government, if it regards war as inevitable even if it does not want it, would be so foolish as to leave to the enemy the choice of time and occasion and to wait for the moment which is most convenient for the enemy."[46] As Glaser and Kaufman point out, "both sides have an incentive to move first, if only to avoid the consequences of letting the other side move first."[47] There are also military objective-based reasons to strike first in space, namely that modern militaries are heavily dependent on space capabilities, so denying or degrading these capabilities first limits the response options an opponent has. Failing to

[42] Glaser, C. and Kaufman, C. (1998), 2.
[43] Townsend, B. (2020), 64-90.
[44] Townsend, B. (2020), 64.
[45] Schelling, T. (1980)
[46] Jervis, R. (1978), 189.
[47] Glaser, C. and Kaufman, C. (1998), 11.

deny these capabilities would result in a state having to "pay a higher cost" later on.[48] Putting an opponent at a disadvantage in their ability to collect intelligence, project forces, communicate, and operate is a significant advantage and is why space systems are believed to be such attractive targets in conflict. All of these factors make space conflict a very real and urgent topic for policy makers, yet the strategies being pursued, like disentanglement, could actually increase the likelihood of attacks even further.

1.2.3 Threats[49]

The United States' potential adversaries recognize that the U.S. military enjoys distinct advantages that are enabled by space systems and therefore disrupting, denying, degrading, or destroying space systems has become an area of focus for foreign governments that seek to limit U.S. advantages in future conflicts. [50] For that reason, many scholars and policy makers believe the question is not *whether* space will be a factor in future conflicts, but *how*.[51] The U.S. relies on space systems to support nearly all warfighting functions and as a result could be disproportionately affected by a conflict in space, compared to other states. This could be a significant motivation for adversaries to attack U.S. space systems, as these attacks could seriously cripple warfighting capabilities.

Aside from the conventional military advantages, potential adversaries, like China, have incorporated space system attacks into nuclear response doctrine to

[48] Morgan, F. (2010), 28-29.
[49] For much more comprehensive review of threats to space systems reference: Harrison, et. al. Space Threat Assessment (2020, 2021) Weeden and Samson, Counterspace Capabilities Assessment (2021); Defense Intelligence Agency, Challenges to Security in Space (2019); and National Air and Space Intelligence Center's Competing in Space (2018).
[50] Moltz, J. (2012), 91-92; Cheng, D. (2012), 58.
[51] Harrison, T., Cooper, Z., Johnson, K., & Roberts, T. G. (2017), 8-9.

overcome space-enabled strategic capabilities, like missile defense.[52] According to Zhang, "many PLA analysts believe that a multilayered ballistic missile defense system will inevitably compromise China's offensive nuclear forces" and threaten China's ability to retaliate against a first-strike by the U.S.[53] As a result, China would need to "weaken American space-based assets such as early-warning satellites, to ensure the credibility of its own offensive nuclear forces."[54] Aside from preserving second-strike capabilities, China could attack NC3 systems in order to achieve information dominance during a conflict. According to Dean Cheng, China's strategy is to "conduct unified operations against an opponent's most important space targets" which are "the key information and space assets which will most affect the enemy's capabilities in the main strategic direction."[55]

Russia has many of the same motivations for attacking NC3 systems as China, and they are far more experienced in the development and fielding of space weapons. Like China, "Russian military thinkers see modern warfare as a struggle over information dominance and net-centric operations that can often take place in domains without clear boundaries and contiguous operating areas."[56] Russia has observed the information advantages space provides to the U.S. military and has developed weapons to "mitigate the superiority of U.S. space assets."[57] Russia has also been more overt in their challenges to U.S. dominance in space. According to the Commander of

[52] A good summary of Chinese views on missile defense can be found in "The China Factor" by Saalman, L (2013), also a great piece on Chinese views of retaliation see Cunningham, F. and Fravel, M. (2015) "Assuring Assured Retaliation."
[53] Zhang, B. (2011), 313, 319, 322.
[54] Zhang, B. (2011), 320; According to Lieber and Press, China's more offensive nuclear posture exists to address peacetime vulnerabilities of an inferior nuclear force. Lieber, K. and Press, D. (2006), 7-34.
[55] Cheng, D. (2012), 69.
[56] Weeden, B., and Samson, V. (2021), xviii.
[57] Weeden, B., and Samson, V. (2021), xviii.

USSPACECOM, General James Dickinson, "Russia publicly claims it is working to prevent the transformation of outer space into a battlefield, yet at the same time Moscow continues to weaponize space by developing and fielding on-orbit and ground-based capabilities that seek to exploit U.S. reliance on space-based systems."[58] Russia's position as a well-armed but declining global power could make for an especially dangerous competitor for the U.S. in space, particularly in light of their aggressive stance toward Ukraine, interference in U.S. elections, hostile cyber activities, and flagrant disregard of prohibitions against the use of chemical and biological weapons.[59] These actions demonstrate a disregard for norms and lack of concern about pressure from the international community.

While China and Russia might be the most widely discussed potential adversaries for the U.S. in a future space or terrestrial conflict, many other nations possess capabilities to target space systems.[60] Figure 1 (below) is from the Secure World Foundation's 2021 Counterspace Capabilities Assessment and provides a useful breakdown of the proliferation and maturity of space weapons capabilities by state. The severity and impact of attacks also varies based on the weapon employed. Some threats permanently destroy systems, while others only temporarily disrupt…and everything in between (see Figure 2 below). While it is not critical for my research to get into specific details about space weapons, it is important to understand that there are real threats to space systems and valid motives to attack space systems in future conflicts. The

[58] U.S. Space Command Public Affairs Office (2020)
[59] Kirby, P. (2022); Goldman, A., Barnes, J. E., Haberman, M., & Fandos, N. (2020); Office of the Spokesperson (2021)
[60] Harrison, T., Johnson, K., & Roberts, T. G. (2019); Secure World Foundation (2021)

willingness of adversaries to attack space systems is what is being investigated in this research, not the ability to conduct such attacks; that has been proven already.

	China	Russia	U.S.	France	India	Iran	Japan	North Korea
LEO Co-Orbital	significant	some	some	none	none	none	none	none
MEO/GEO Co-Orbital	some	none	none	none	none	none	none	none
LEO Direct Ascent	significant	some	some	none	some	none	none	none
MEO/GEO Direct Ascent	some	some	some	none	none	none	none	none
Directed Energy	some	some	some	some	none	none	none	none
Electronic Warfare	significant	significant	significant	some	some	some	none	some
Space Situational Awareness	significant	significant	significant	some	some	some	some	none

Legend: none some significant

Figure 1 - Counterspace Capabilities Assessment by Country[61]

Figure 2 - Counterspace Continuum[62]

[61] Secure World Foundation. (2021).
[62] Defense Intelligence Agency. (2019), 36.

Several countries possess directed energy weapons like lasers and high-powered microwaves.[63] These systems can be used to rapidly generate effects that can be either temporary in nature or permanently damage spacecraft components. Lasers, for example, could be employed to temporarily blind an ISR or missile warning sensor, or they could potentially permanently degrade the sensor. Nuclear weapons can also be detonated in space or in the atmosphere to create an electro-magnetic pulse (EMP). EMPs can cause electronics that are not properly shielded to fail. The U.S. conducted nuclear detonations in space in 1962 with the Starfish Prime experiments that resulted in EMPs that blacked out Oahu hundreds of miles below. Nuclear detonations in space were later prohibited by the Limited Nuclear Test Ban Treaty, but the capability to conduct such attacks still exists.[64]

While most people focus on ASATs and directed-energy weapons when space weapons are discussed, they actually represent only a fraction of counterspace systems. When the full range of weapons is considered, it is not appropriate to say that space weapons have never been used in anger.[65] There are many historical cases of intentional satellite jamming, including jamming by Russia in support of their operations in Ukraine, as well as by the U.S. in support of previous military campaigns.[66] GPS jamming is also extremely common around the world and even long-haul truckers have employed localized GPS jammers to conceal their location, speed, and other information from

[63] Weeden and Samson (2021) and Harrison et al. (2021) provide extensive background on non-kinetic weapons including current status and numbers of lasers and directed energy weapons employed by various countries.
[64] King, G. (2012, August 15). Going Nuclear Over the Pacific. Retrieved from Smithsonian Magazine: https://www.smithsonianmag.com/history/going-nuclear-over-the-pacific-24428997/
[65] Amenbar, C. (2020, July 23). Counterspace Weapons 101. Retrieved from Center for Strategic and International Studies: https://aerospace.csis.org/aerospace101/counterspace-weapons-101/.
[66] Velkovsky, P., Mohan, J. and Simon, M. (2019); Howell, E. (2022).

interested parties.[67] Larger jammers that can affect systems within hundreds or thousands of meters have been employed by insurgent groups and states alike and are very simple and inexpensive to build. These types of systems are widely proliferated and constitute a serious threat, but mitigations and systems to counter these threats have also been deployed.

A pervasive and rather intractable problem is that nearly all space systems are vulnerable to a host of cyber threats. Cyber weapons can be used to take over C2 of satellites, disable ground infrastructure, corrupt data, disable networks, hijack dissemination or many other malicious actions. Cyber threats are extremely dangerous because of the near-instantaneous speed of attack, difficulty in attribution, and the relative ease of access to the cyber domain for states and non-state actors alike. In 2007 and 2008 the U.S. believes China hacked into NASA environmental monitoring satellites, though the attacks were never publicly acknowledged.[68] States or other actors that cannot or choose not to deny U.S. space capabilities through high-tech or high-cost applications like ASATs or directed-energy weapons can potentially achieve the same (or better) results through cyber attacks. Cyber attacks could present an adversary with the opportunity to instantaneously disable critical space systems while not affecting their own systems, not generating a highly attributable signature, and potentially at a fraction of the cost of other weapons. It could reasonably be concluded that cyber threats pose the gravest danger to space systems today.

---

[67] Brewin, B. (2013, August 8). Every Three Years Someone Gets Busted for Using a GPS Jammer. Retrieved from Nextgov: https://www.nextgov.com/cio-briefing/2013/08/every-three-years-someone-gets-busted-using-gps-jammer/68348/.

[68] Arthur, C. (2011, October 27). Chinese hackers suspected of interfering with US satellites. Retrieved from The Guardian: https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected

1.3 Framing the Problem: Deterrence and Inadvertent Escalation

To counter the many threats that plague the space domain today, the United States has prioritized deterrence and the 2020 Defense Space Strategy lists deterring aggression in space as the top priority.[69] Unfortunately, according to many space security scholars "the U.S. has not communicated a clear space deterrence framework to adversaries" and overall deterrence in space is "low."[70] Additionally, the DoD has identified the need to shape perceptions and define responsible behavior in space in order to reduce the risk of miscalculation, mishaps, and misperception.[71] Yet, responsible behavior has not been defined, norms have not been established, and the lack of cooperation that "might promote mutual restraint" has created a Wild West of sorts in the space domain. [72] Without existing policies, norms, red lines, or threats to inform decision makers in space-faring states, perceptions and misperceptions become even more critical. One area of possible miscalculation and misperception that has received recent attention in academic circles is the entanglement of NC3 systems. Despite efforts to deter, adversaries could be willing to attack space systems to achieve military or political objectives, and this could include attacks against entangled NC3 space systems, even in lower-level conventional or regional conflict. As a result, some scholars argue that entangled NC3 systems could carry a significant risk of inadvertent escalation.[73]

---

[69] Office of the Secretary of Defense. (2020, 2.
[70] Mallory, K. (2018). New Challenges in Cross-Domain Deterrence. Santa Monica, CA: RAND Corporation, 8. and Harrison, T., Cooper, Z., Johnson, K., & Roberts, T. G. (2017). Escalation and Deterrence in the Second Space Age. Washington, DC: Center for Strategic and International Studies, 30-31, 135.
[71] Office of the Secretary of Defense. (2020), 8.
[72] Moltz, J. C. (2012). Asia's Space Race. New York, NY: Columbia University Press, 13.
[73] Morgan, F. E. (2010). Deterrence and First-Strike Stability in Space. Santa Monica, CA: RAND Corporation, xi.; Acton, J. M. (2018). Escalation through Entanglement. International Security, 92-95.; Townsend, B. (2020). Strategic Choice and the Orbital Security Dilemma. Strategic Studies Quarterly, 78.

The body of literature that addresses the risks of inadvertent escalation as a result of nuclear/conventional entanglement extends across the space and terrestrial domains.[74] Barry Posen asserts that "direct conventional attacks on critical nuclear forces, attacks that degrade strategic early warning or command and control systems, or even attacks on general-purpose forces that protect strategic nuclear forces, could all produce strong reactions from the party on the receiving end."[75] These "strong reactions" could include anything from elevated alert status to nuclear retaliation.[76] James Acton, Forrest Morgan, and Brad Townsend all apply this logic specifically to space systems and assert that entangled NC3 space systems are attractive targets, even in conventional and/or regional conflicts, and that attacks against entangled systems in these cases could lead to inadvertent escalation.[77] Similar claims about entangled systems outside of the space domain have been made by a number of scholars, including Rovner, who says that "inadvertent escalation may occur when conventional attacks put the adversary's nuclear force at risk."[78]

Recently, however, other scholars have challenged the logic of inadvertent escalation as a result of entanglement. Echoing Posen's acknowledgement that "we have no examples of such escalation," Kroenig and Massa reinforce that "there is no evidence of dual-capable systems ever producing nuclear escalation in the empirical record."[79] Kroenig and Massa also claim that the hypothetical escalation cases generated by entanglement theorists previously are "logically inconsistent, lack strategic empathy, and

[74] Acton, J. (2020); Tannenwald, N. and Acton, J. (2018); Rovner, J. (2017); Arbatov, A. et al. (2017); Posen, B. (1991).
[75] Posen, B. (1991), 3.
[76] Posen, B. (1991), 4-5.
[77] Acton, J. (2018); Townsend, B. (2020); Morgan, F. (2010)
[78] Rovner, J. (2017), 702.
[79] Posen, B. (1991), 4; Kroeinig, M. and Massa, M. (2021), 1.

do not account for operational obstacles to nuclear preemption."[80] Kroenig and Massa do not specifically address NC3 space system entanglement in their work, but they do agree that entanglement could produce a deterrent effect because "leaders might conclude that attacking dual-use capabilities is too risky."[81] The potential deterrent value of entanglement also surfaces in Government Accountability Office (GAO) reports about the DoD's plans to disentangle NC3 space systems.[82] Ultimately, the decision to entangle or disentangle is about managing risk, but risks cannot be appropriately considered without data. That is the gap my research attempts to fill.

1.3.1 Disentanglement and Deterrence

Unfortunately, decisions about entanglement have already been made without data. In order to address the perceived risks of inadvertent escalation and to enhance resilience, the DoD has committed tens of millions of dollars toward disentangling (or disaggregating in DoD terms) the NC3 space architecture.[83] Senior policy makers in the U.S. Government are being encouraged to "embrace disaggregation" and focus on separating nuclear and conventional missions from NC3 space systems.[84] The most current Joint Publication for Space Operations, JP 3-14 advocates for the separation of "tactical and strategic protected SATCOM," which are some of the NC3 systems I investigate.[85] Military space leaders claim that "disaggregation is an innovative opportunity to stay ahead of our adversaries, to change their targeting calculus, and to mitigate the effects of a widespread attack on our space assets."[86] With the lack of

[80] Kroenig, M. and Massa, M. (2021), 3.
[81] Kroenig, M. and Massa, M. (2021), 12.
[82] Government Accountability Office (2015).
[83] Erwin, S. (2021); Government Accountability Office (2019), 3-4.
[84] Taverney, T.D. (2011).
[85] Joint Chiefs of Staff (2020), I-9.
[86] Air Force Space Command (2016), 10.

historical evidence to support inadvertent escalation through entanglement, the lack of empirical testing of entanglement as a deterrent, and the potential costs and risks associated with disentanglement (namely an increased likelihood of attack against disentangled conventional systems), why is the DoD continuing down this path?

The DoD provides a number of reasons why it believes disaggregating/ disentangling NC3 space systems is a good strategy. One of the primary arguments is that disentanglement will lead to increased resilience. Resilience is defined as "the ability of a system architecture to continue providing required capabilities in the face of system failures, environmental challenges or adversary challenges."[87] Many scholars have argued in favor of space system resilience not just because a resilient architecture could preserve capability in the face of an attack, but also because resilience could reduce the benefits to an adversary of conducting an attack, and therefore strengthen deterrence through denial.[88] Disentanglement is said to contribute to resilience in the sense that a greater number of, and more widely dispersed, network of satellites allows for an increased ability to withstand attacks and anomalies. This could very well be true, but it ignores the critical fact that resilience and entanglement are not mutually exclusive.

Entangled systems can also be made more resilient by increasing the number, types, and location of systems. It is not necessary to separate nuclear and conventional missions to develop resilient architectures; the systems could remain entangled while being made more resilient. By using different terms and concepts interchangeably, the DoD has inadvertently obscured the fact that disentanglement alone does not automatically boost resilience, and entanglement does not decrease resilience. Resilience

[87] Hastings, D.E. & La Tour, P.A. (2016).
[88] Macdonald, B. (2013), 84-86; Harrison, T., Cooper, Z., Johnson, K., & Roberts, T. G. (2017), 32.

is a strategy that could (and probably should) be used regardless of whether or not systems are entangled. Claiming that disentanglement is necessary for resilience in NC3 architectures is patently false.[89]

Moreover, resilience might not actually be as strong of a deterrent as scholars have asserted. Space system resilience as a mechanism of deterrence (agnostic of entanglement) has been empirically tested previously. During space security tabletop crisis scenarios conducted by the Center for Strategic and International Studies (CSIS), researchers found that "resiliency was a significant advantage for those teams who had secondary systems or were able to work around the loss of capability."[90] However, resilient space systems were still attacked during the scenarios. Even when attackers were unable to weaken or degrade opponent capabilities as a result of resilient architectures, they still chose to attack these systems. This finding calls into question assumptions about the effectiveness of resilience as a deterrence by denial strategy. If the DoD's ultimate goal in space is deterrence, attacks against resilient systems should not be viewed as more tolerable simply because some capabilities are protected in the immediate term. The goal should still be to deter attacks from occurring in the first place, and the existing research shows that this cannot be done with resilience alone.

The DoD also believes that disentanglement will enhance deterrence by "increasing the number and diversity of potential targets, thereby complicating an adversary's decision calculus and increasing the uncertainty of successful attack."[91]

---

[89] There are dozens of proposed methods for space system resiliency. For a good summary of resilience measures, reference the 2015 Space Domain Mission Assurance report from the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security.
[90] Harrison, T. et al. (2017), 43.
[91] Air Force Space Command (2016), 2-3.

Again, this speaks more to resilience than disentanglement, because entangled architectures could also include higher quantities and greater diversity of satellites. Launching more entangled satellites and spreading them out across different orbits can still achieve resilience without separating the nuclear/conventional missions of these systems, so this line of reasoning is faulty. Another claim is that disentangling NC3 systems would contribute to deterrence by signaling that "some missions such as nuclear attack warning would be understood to be clearly "off limits," or the aggressor would risk nuclear escalation."[92] Here, senior military space leaders confirm that nuclear escalation could occur in response to attacks against NC3 space systems. Disentangled nuclear attack warning (missile warning) satellites should be safer from attack, but what of the conventional versions of the systems? It sounds like these leaders are conceding that conventional systems will not be "off limits." Also, if limits and threats can be effective for the nuclear systems, why not choose to keep nuclear/conventional missions together to protect both missions? Is deterrence across the space domain the DoD's goal, or only deterrence for nuclear systems? Finally, this statement assumes that adversaries can be made aware of which systems are part of the strategic/nuclear architecture (and which are not), and that threats would be both believed and accepted. If this is the case, why is disentanglement needed to begin with?

Another justification for disentanglement is that it "may help mitigate the risk of uncontrolled escalation during crisis or conflict without necessarily bolstering resilience."[93] This speaks to the fears presented by Posen, Acton, and others about inadvertent escalation as a result of entanglement. However, this is an untested

[92] Air Force Space Command (2016), 9.
[93] Office of the Assistant Secretary of Defense for Homeland Defense and Global Security. (2015), 6.

hypothesis and there is nothing that mandates "uncontrolled escalation" for attacks on entangled systems, nor anything that proves inadvertent escalation will not occur with disentangled systems. This line of reasoning that disentangled systems incur differing responses to attacks is exactly what I point to in asserting the deterrence value of entanglement. Adversaries must be willing to confront the real possibility of "uncontrolled escalation" and that is exactly what makes deterrence effective.

The DoD's claims about disentanglement as a deterrence strategy are soundly rooted in deterrence by denial theory, which asserts that if the attack being considered is unlikely to achieve the desired objective, then a decision maker should be deterred from conducting such an attack.[94] However, as I mentioned previously, these claims are more about resilience than entanglement, and resilience can be achieved with entangled architectures as well. The DoD has also failed to consider how entanglement could actually provide significant deterrence value, while disentanglement could be riskier. By attacking entangled systems, even in a conventional or lower-level conflict, adversaries could be subject to a much more severe and costly retaliation than they would otherwise be willing to accept to achieve their objectives if systems were disentangled. Using Air Force Space Command's words, why wouldn't these entangled systems be clearly "off-limits" if they are performing strategic nuclear functions? Do the conventional missions these systems support really make the strategic functions of the systems fair game for adversaries? Again, if the DoD's goal in space is deterrence, how does disentanglement not make that proposition more unrealistic?

[94] This concept is widely covered in deterrence theory literature, see George and Smoke (1974); Schelling (1966, 1980); Jervis (1979).

I am not the first to challenge the DoD's assumptions in this area. In a 2014 report, the Government Accountability Office (GAO) shared many of these concerns about the DoD's push toward disentanglement. According to the GAO, the most serious risk of disentangling is that "adversaries may be more likely to attack small tactical satellites because they may be viewed as lower risk with regard to escalating hostilities."[95] Additionally, the report states that launching more satellites with different functions increases the challenge of defending these systems, while also adding more debris and objects into an already crowded environment. Further, a capable adversary might still be able to target large, disentangled constellations by attacking C2 nodes or other infrastructure, or the satellites themselves. Finally, if disentanglement is pursued "strategic payloads may no longer be able to support multiple missions, and tactical payloads may lose some of the protection provided by radiation-hardened strategic satellites."[96] The GAO noted that studies performed by the DoD did not "comprehensively assess the effects of disaggregation" and that previous DoD reports lacked measures of effectiveness to evaluate these decisions.[97] According to the GAO, the DoD focused more on technical feasibility than operational impact, which is alarming considering the criticality of these systems and what disentanglement could mean if the DoD's assumptions are incorrect.

1.4 Relevance

For the average person, space is often thought of as little more than a frontier for exploration or a setting for science-fiction entertainment. However, the impact of space

[95] Government Accountability Office (2014), 11.
[96] Government Accountability Office (2014), 11-12.
[97] Government Accountability Office (2014), 12

on our modern way of life cannot be overstated. According to the National Academy of Sciences:

> "The list of human activities that are dependent on space systems contains most of the major functions that are vital to modern society, including trade and commerce; banking and financial transactions (from operations of major financial markets to minor retail purchases); personal, corporate, and government communications; agriculture and food production and distribution; power and water systems; transportation; news gathering and distribution; weather assessment and prediction; health care and entertainment. Were the world to suddenly be "without space," these would all seriously degrade or shut down entirely."[98]

Preserving peace in space is critical, and the peaceful use of space extends far beyond preserving military advantages for the United States and its allies. A space war could totally cripple the global economy and critical infrastructure and "the aftermath of space warfare could be equivalent to that of a nuclear war."[99] Army Major General Thomas James, Commander of the Joint Task Force for Space Defense at USSPACECOM, summed up the issue quite succinctly by stating that "no one wins if war extends into space."[100] It is essential, therefore, that we treat space with the same careful consideration with which we address other strategic issues of global importance.

Senior military leaders caution against the belief that the absence of space warfare in the past, and the factors that led to peace, predict a peaceful future. They claim that new mechanisms for deterrence and space security must be pursued as the number and capabilities of actors in space increase rapidly.[101] It is true that the international environment has changed dramatically since the Cold War, and despite the intense

[98] Committee on National Security Space Defense and Protection. (2016, 2.
[99] Dawson, L. (2018), 157.
[100] Seligman, L. (2019).
[101] AFSPC (2016), 2, 10.

competition between the U.S. and the Soviet Union, the bipolar environment of the Cold War made competition in space simpler. According to space security scholar James Clay Moltz, "the higher "transaction costs" required to craft and enforce multilateral agreements make space management today arguably much more difficult."[102] Space is no longer a domain just for the wealthiest and most powerful states, nor are activities in space restricted only to states. However, space warfare is a foregone conclusion, and with the right mix of policies and strategies, deterrence is still possible.

With this in mind, my research has the potential to influence policy decisions regarding the U.S. NC3 space architecture, or at the very least shed light on some of the possible outcomes of these policy decisions and provide data for decision makers to weigh options more effectively for future space acquisitions programs. In addition to being relevant to current space policy, my research also attempts to fill theoretical gaps in our understanding of deterrence in space; particularly how perceptions of space systems and expected punishments influence adversary decision making. Finally, my research adds empirical analysis to existing theoretical work regarding entanglement. Current hypotheses about the effects of entanglement are entirely speculative, and my research is the first to isolate and test entanglement as an independent variable. With millions of dollars, the sanctuary of space, and national security on the line, untested assumptions about the benefits of disentanglement are insufficient and quite frankly dangerous.

1.5 Summary of Findings

The findings offer mixed support to my theory of deterrence through entanglement. In the space security wargames I conducted with students at Georgia Tech,

[102] Moltz, J. C. (2012), 13.

entanglement played a significant role in deterring attacks against NC3 space systems compared to disentangled systems. Entangled teams were also less likely to conduct attacks of any type during the wargames. Of the 20 teams that did not conduct any type of attack during the wargaming sessions, 18 were entangled teams. Additionally, when entangled teams did conduct attacks, they were more likely to use less destructive temporary non-kinetic weapons compared to disentangled teams. The wargames also demonstrated a greater willingness to attack conventional versions of disentangled systems due to the perceived lower retaliation costs. Entangled systems were attacked an average of 0.42 times per team, compared to 1.38 attacks per disentangled team, and 2.08 attacks for teams that were unaware of entanglement. Disentangled nuclear systems were attacked least of all, with an average of 0.15 attacks per team. Overall, the wargame findings provide strong support to my theory of deterrence through entanglement.

The findings from the elite surveys, however, do not provide such strong support the theory, at least not entirely. Survey respondents in the entangled systems treatment were slightly more likely to attack NC3 space systems than their disentangled counterparts, though the differences were not statistically significant. That said, entangled respondents did state that missile warning systems should not be attacked to avoid escalation, and no attacks were conducted on missile warning systems by respondents in this group. Disentangled respondents also showed a greater willingness to attack conventional versions of disentangled systems, including missile warning, but ultimately were less likely to conduct attacks in general. Like the wargames, disentangled nuclear systems were safest from attack, with only one respondent choosing to target these systems. One of the more interesting findings from the elite surveys is that respondents

expected less severe retaliation for attacks they conducted on adversary systems than for the same attacks conducted on their systems. This indicates a disparity in expected costs of attacks based on whether the state is the attacker or victim, which could be a blind spot for states conducting a cost-benefit analysis of whether or not to attack.

Finally, the public sample survey again failed to yield statistically significant differences across entanglement treatments, though respondents with entangled systems were more likely to support harsher responses than those with disentangled systems. Again, there were significant differences in the perceived severity between attacks against disentangled conventional and disentangled nuclear systems, with the former necessitating less severe retaliation. Overall, the public survey demonstrated that public support for retaliation in response to space system attacks is largely based on what type of attack occurred, more than any other factor. Public respondents were more likely to favor proportional responses across all entanglement treatments and supported much more severe retaliation for kinetic attacks versus non-kinetic. This was a common theme across all experimental methods. In the wargames and surveys, participants preferred to employ non-kinetic weapons, particularly cyber weapons. In addition to the willingness to use these weapons, participants generally viewed cyber attacks as being less severe than other types of attacks when they were on the receiving end. This preference for cyber attacks and lower cost of use could signal important trends for the future of space conflict.

1.6 Moving Forward

The next chapter of this dissertation covers my theory of deterrence through entanglement by incorporating and building upon deterrence, entanglement, and space

security literature. In addition to laying out my theoretical argument, the chapter provides scope conditions for the theory and identifies the variables and hypotheses I test with my experimental research methods. Chapter 3 describes my research approach and provides justification for the wargames and surveys I conducted. Chapter 4 is the first of the empirical chapters and discusses the design, implementation, and results of the space security wargames. Chapter 5 presents the surveys conducted with elites from the military space operations community, as well as a public opinion survey conducted with workers from Amazon's MTurk online labor market. Finally, Chapter 6 provides a brief summary, as well as conclusions, policy recommendations, and goals for future research.

CHAPTER 2. THEORY

"A fine deterrent can make a superb target." - Thomas Schelling[103]

2.1 Background

Space weapons could diminish asymmetric advantages of states that are heavily dependent on space for their military operations, like the United States.[104] As a result, many space security scholars and military planners have concluded that offensive space capabilities are likely to be employed in future conflicts. The prevailing belief throughout academia and the defense establishment is that NC3 space systems are particularly likely to be attacked in future conflicts due to the broad range of warfighting capabilities these systems provide.[105] These low-density and high-value assets are considered "juicy targets" for potential adversaries who are aware of how critical these systems are for the United States and its ability to wage war.[106] In order to reduce the appeal of these juicy targets and decrease risk of inadvertent escalation, the DoD has advocated for disentangling (or disaggregating in the DoD parlance) the U.S. NC3 space architecture.[107] According to Air Force Space Command (now the U.S. Space Force) disentangling space systems, specifically NC3 systems, complicates an adversary's cost-benefit analysis, and by doing so contributes to deterrence.[108] Disentangling is also said to reduce the risk of

[103] Wohlstetter, R. (1962). Pearl Harbor: Warning and Decision. Stanford, CA: Stanford University Press, vii-viii.
[104] Harrison et al. (2017, 2019, 2020, and 2021); Moltz, J. (2008, 2012, and 2014); Cheng, D. (2012); Hyten, J. (2016); Shelton, W. (2017); Johnson-Freese, J. (2017); Klein, J. (2006); Defense Intelligence Agency (2019); National Air and Space Intelligence Center (2018).
[105] Cheng, D. (2012); Acton, J. (2018); Arbatov, A., Dvorkin, V. and Topychkanov, P. (2017); Zhang, B. (2011); Zhao, T. and Bin, L. (2017); Air Force Space Command (2016); Defense Intelligence Agency (2019); National Air and Space Intelligence Center (2018)
[106] Erwin, S. (2017)
[107] Joint Chiefs of Staff (2020); Air Force Space Command (2016); Office of the Assistant Secretary of Defense (2015); Government Accountability Office (2014)
[108] Air Force Space Command (2016)

inadvertent escalation and provide greater flexibility in managing escalation. For these reasons, the current strategy for the U.S. is to pursue disentanglement, and tens of millions of dollars have been spent toward this end.[109]

However, these assumptions have never been observed in the real world nor empirically tested in an experimental setting. I argue that entanglement actually deters attacks against NC3 systems due to the severe consequences an adversary should expect in response to attacks that degrade vital nuclear capabilities of a targeted state. I also argue that disentanglement raises the likelihood of attacks against space systems due to the perception that the consequences of attacks against conventional systems will be less severe. I test this theory using experimental wargaming scenarios and elite surveys that isolate entanglement as an independent variable, which has never been accomplished previously. I assess the effects of entanglement through my dependent variable deterrence, which I measure by using attacks against space systems as a proxy.

Space is integral not only to modern military operations, but to the conduct of modern life as well. Unfortunately, space security has not received widespread attention from the IR community historically and strategies are being pursued within the DoD, like disentanglement, which could have unintended strategic consequences. In an anarchical system, states attempt to increase their control "over those aspects of the international system that make its basic values and interests more secure."[110] However, sometimes these well-intentioned actions ultimately result in decreased security. The U.S. and others have developed offensive and defensive space weapons and are pursuing strategies like disentanglement to gain control over the space domain, or at the very least increase their

[109] Government Accountability Office (2015 and 2019); Erwin, S. (2021)
[110] Gilpin, R. (1981), 50.

odds of success in a conflict that extends to space. However, by attempting to increase their own security, states decrease the security of others and can ultimately make themselves less secure.[111]

These strategies could worsen the already tense situation in space, which is growing increasingly unstable for a few reasons. One, space is viewed as an offense-dominant domain, meaning that it is easier to attack in space than defend, and that adding offensive capabilities is cheaper than adding defensive capabilities.[112] Additionally, space weapons are most useful in a first-strike application because attacking space capabilities could degrade an adversary's ability to retaliate, since their own retaliatory actions would rely on space.[113] If war is imminent, it is in the best interest of a militarily inferior state to diminish the capabilities of their adversary first, and denying or degrading space capabilities could be decisive in that regard. Finally, the existing orbital security dilemma has created volatility in the space domain that has increased competition among space-faring states and created a sense of urgency for policy makers. All of these factors reduce stability and fuel arms racing and aggression.[114] Without norms or coherent deterrence strategies in place, the likelihood for misperception and miscalculation in space is at an all-tine high. Thus, the need for effective deterrence strategies in the space domain is also at an all-time high. Yet the disentanglement strategy the U.S. is pursuing could ultimately make space less stable and less secure for all actors by signaling that the U.S. is preparing for war in space while simultaneously lowering the expected costs and risks of attacks.

---

[111] Jervis, R. (1978)
[112] A number of scholars have written about the assumed offense dominance of the space domain. See Finch, J. & Steene, S. (2011), 11; Harrison, R., Jackson, D., & Shackleford, C. (2009), 6; Manzo, V. (2011), 3; Morgan, F. (2010).
[113] Morgan, F. (2010); Finch, J., and Steene, S. (2011), 10-17.
[114] Glaser, C. and Kaufman, C. (1998), 2.

No prior research has investigated the effects of entanglement on deterrence and stability in the space domain; this research aims to address this gap in understanding.

In this chapter, I present my theory of deterrence through entanglement and discuss the scope and constraints within which my theory is situated. From there, I cover some of the existing literature on deterrence as it relates to my theory and describe my use of deterrence as the dependent variable for my research. Next, I review literature and theories on entanglement, including space system entanglement, and present entanglement as my independent variable. At the end of the chapter, I discuss some of the counter arguments to my theory as well as provide a brief summary.

2.2 Theory Scope/Constraints

Before going any farther, it is important to set boundaries on who and what my theory applies to. As far as who, the theory I present applies to the range of actors that operate in space and possess the capability to identify, target, and attack NC3 space systems. Because this theory specifically addresses willingness to attack space systems, the states considered must have the capability to attack in order to be deterred from doing so. A much larger sample of actors could be included based on the ability to conduct cyber attacks, however, the exquisite intelligence required to target NC3 space systems makes attacks originating from states or groups that do not possess robust space situational awareness (SSA) capabilities unlikely. The primary threats to U.S. NC3 space systems come from China and Russia, and in the Chinese and Russian view, the U.S. poses the primary threat to their space systems and NC3 architectures.

My theory is predicated upon awareness of both the entanglement status of a state's NC3 systems, as well as any publicly stated policies or threats regarding attacks

against space systems. Deterrence depends on clearly communicated credible threats, so adversaries must be aware not only of the capabilities a state possesses to retaliate, but also some expectation of the severity placed on attacks against space systems. States included in this theory are aware or can be made aware of entanglement as well as policies for retaliation. If a state possesses the capability to target a spacecraft, it should also have the ability to determine the type and capabilities of the spacecraft being targeted (as in whether the system is entangled or not). Operating space systems is a complex, technical, and precise endeavor, and targeting space systems is even more complicated. It is unreasonable to assume that a system would be attacked without the attacker understanding the function and capabilities of that system, unless the true nature of a system differed from what could be observed. NC3 space systems are large, exquisite, and have easily tracked orbits and easily identifiable features. A capable adversary could determine the location and function of these systems with moderately sophisticated space situational awareness capabilities.

It is possible that an adversary could be aware of the mission of a satellite without knowing that the system is entangled, and there is some discussion in the literature about states potentially attacking NC3 space systems without awareness of entanglement.[115] However, this can be countered by looking at the DoD's claims about disentanglement. If the U.S. believes that disentanglement can contribute to deterrence, which would require adversaries being aware of disentanglement, then we must also accept that they could be made aware of entanglement, if they are not already. Additionally, Chinese and Russian writings on the subject make it clear that both states are aware of NC3 system

[115] Acton (2018), 66-70.

entanglement, though their perspectives on the matter differ.[116] More on that topic will be covered in the entanglement section of this chapter. To summarize, this theory applies to states that have the capability to hold space systems at risk and who are aware or can be made aware of both the entanglement status of space systems and policies or threats relating to attacks against those systems.

Less clear, to both adversaries and states operating NC3 systems, is what should be expected in response to attacks against these systems. All states that operate NC3 space systems also have robust capabilities to hold adversaries at risk and make good on threats, including nuclear threats. Yet none of the states have specifically identified what type of response could be expected, and there is significant disagreement about the credibility of threats in response to attacks against space systems.[117] This disagreement, particularly amongst U.S., Chinese, and Russian scholars will be discussed later in the chapter, but as it relates to the scope of my theory, the point is that I assume states are aware or can be made aware of threats, policies, or thresholds. Again, I refer to the DoD's own argument for disentanglement in which the claim is that "some missions such as nuclear attack warning would be understood to be clearly "off limits."[118] In this instance, Air Force Space Command is referring to the nuclear/strategic versions of disentangled systems, which actually supports my argument. If adversaries can be made aware that disentangled nuclear systems are off limits, adversaries could also be made aware that entangled NC3 space systems are "off limits." Whether or not adversaries perceive the latter argument to be true is what I investigate. The DoD's claim about nuclear systems

[116] Arbatov, A., Dvorkin, V. and Topychkanov, P. (2017); Zhao, T. and Bin, L. (2017)
[117] Lewis, J. (2013); MacDonald, B. (2013); Klare, M. (2019); Arbatov, A., Dvorkin, V. and Topychkanov, P. (2017); Zhao, T. and Bin, L. (2017)
[118] Air Force Space Command (2016), 2-3.

being off limits also sends the message that non-nuclear systems are not off limits, which supports my hypothesis that these systems are more likely to be attacked.

Finally, I need to address what level of deterrence I am claiming with my theory. Deterrence through entanglement refers specifically to deterring attacks against entangled space systems. While it could be possible that entangled NC3 systems might provide some broader deterrence value, I am not investigating that directly through my research. An often-cited scenario in which U.S. NC3 space systems could be attacked is a Chinese invasion of Taiwan.[119] In this scenario, China could attack U.S. NC3 space systems not only to reduce the visibility of their actions, but to hinder the U.S.' ability and willingness to project military capabilities forward. If China believed it was necessary to attack U.S. NC3 systems in order to carry out a successful invasion of Taiwan, then deterring attacks against NC3 systems could more broadly contribute to deterring the invasion altogether. Said differently, if attacking NC3 space systems was a requisite for invasion, but the cost of attacking these systems was higher than the expected benefits of the invasion, then the deterrence value of the NC3 systems would be extended beyond just preserving those systems and their capabilities. This is purely hypothetical, and my theory does not address deterrence beyond the level of the space systems themselves. The table below summarizes the scope and constraints of my theory covered in this section:

[119] Zhao, T. and Bin, L. (2017), 52.

Table 1 - Scope of Theory of Deterrence through Entanglement

States Included	Requisite Capabilities	Requisite Awareness	Level of Deterrence
- United States - China - Russia - France - India - Iran	- Capability to attack NC3 space systems - Ability to credibly threaten punishment	- Entanglement status of NC3 space systems - Policies for attacks against NC3 space systems - Severity of consequences for attacks	- Attacks against NC3 space systems[120]

2.3 Argument and Hypotheses

My theory of deterrence through entanglement operates on two key premises. First, severe retaliation (reaching a level that is unacceptable to an attacker) is more likely and credible when a nation's most critical assets are at stake, particularly nuclear assets. Therefore, potential adversaries should be deterred from attacking vital nuclear assets of other states. Entangled NC3 space systems are considered vital nuclear assets, so from this logic I present my first hypothesis: *H1: Entanglement deters attacks against NC3 space systems.* [121] On the other end of this claim, disentangled conventional systems are less likely to incur severe punishment and/or invite uncontrolled escalation. Therefore, these systems could be more attractive targets to adversaries. This leads to my second hypothesis: *H2: Disentanglement of NC3 space systems makes attacks against conventional versions of the disentangled systems more likely.*

[120] In addition to the actual number of attacks, I argue that any attacks against entangled NC3 systems will be less severe (using temporary, non-kinetic means) compared to attacks against disentangled systems.
[121] The nuclear/strategic versions of disentangled systems are considered vital nuclear assets and attacks against these systems should also be deterred.

My theory and hypotheses are centered upon the notion that an adversary's cost/benefit calculus is contingent upon their perception of punishment and that entanglement incurs both a more severe and higher likelihood of punishment in response to attacks than disentanglement. Deterrence through entanglement works by keeping expected costs above the expected payoff threshold. Writing about NC3 systems during the Cold War, Krepon says that "attacks on critical assets and infrastructure in space commonly were viewed in the gravest terms, regardless of whether they were precursors to attacks on nuclear forces" and "these conditions continue to remain in place."[122] As mentioned in Chapter 1, NC3 space systems sit atop the hierarchy of criticality and attacks against these systems could justify nuclear retaliation. Potential attackers are forced to contend with the prospect that attacks against entangled NC3 space systems could be met with the gravest possible response.

There is a possible credibility gap at play here, as it might be hard to imagine the use of nuclear weapons in response to attacks against satellites, but as Thomas Schelling so poignantly contends in *Arms and Influence*, this is a "threat that leaves something to chance."[123] According to Jervis, "there is an irreducible minimum of unpredictability that operates, especially in situations which engage state's highest values" and even if a nuclear response is unlikely or seemingly irrational "the mere possibility may be an effective deterrent."[124] George and Smoke argue that "instead of emphasizing the critical importance of credibility and signaling to deterrence strategy, theorists would do better to caution that sophisticated opponents will judge credibility on the basis of a more

[122] Krepon, M. (2013)
[123] Schelling, T. (1966)
[124] Jervis, R. (1979), 299-300.

fundamental analysis of the defender's interests."[125] NC3 space systems are among a defender's most vital interests.

For the second part of this argument, an adversary is unlikely to expect the same severity of consequences for attacks against disentangled conventional systems, and therefore the cost/benefit calculus could justify an attack. This reasoning draws partially from the stability/instability theory which asserts that nuclear capabilities might prevent all out nuclear war, but they actually have a destabilizing effect in the conventional realm and could make conventional attacks more likely.[126] "The less likely a conventional war is to escalate to a nuclear war, the lower the expected cost of launching a conventional war and the more likely states are to start them."[127] Disentangled systems allow for a greater assurance that attacks can occur against conventional versions of these space systems without escalating to the level of full-scale or nuclear war. An adversary could use the greater escalation flexibility offered by a disentangled architecture to their advantage and feel safer conducting attacks against conventional systems.

Adversaries are deterred from attacking entangled systems because attacks incur the risk of severe and possibly nuclear retaliation and uncontrolled escalation. These risks outweigh the possible benefits of denying, degrading, disabling, or destroying the NC3 system. My theory is based upon how aggressors perceive threats and risks, and how these perceptions affect their decision making. As will be discussed later in this Chapter, some experts believe NC3 space systems can be attacked without fearing a severe retaliation. They view attacks against NC3 space systems as legitimate options to achieve

[125] George, A. and Smoke, R. (1974), 560.
[126] Krepon, M. (2004); Rauchaus, R. (2009); Watterston, C. (2017)
[127] Powell, R. (2015), 596.

conventional or tactical objectives.[128] Others believe nuclear retaliation to be a credible threat for attacks against NC3 space systems, and that attacks against NC3 systems should be avoided in any circumstance outside of total war.[129] Both beliefs are valid and both might be true based on the actor and context of the situation, but how these beliefs translate to actual decision making and deterrence has never been empirically tested before. That is the gap I attempt to fill with my research.

2.4 Deterrence

2.4.1 Why States Attack

In constructing a theory of deterrence, it is important to first consider that states have myriad reasons for conducting attacks against other states and initiating war. Perhaps the most parsimonious explanation for why states attack and go to war with other states is that these actions are the result of "international anarchy, combined with states' uncertainty about each other's motivations."[130] Some of the rational explanations for why states choose to go to war include: "(1) anarchy; (2) expected benefits greater than expected costs; (3) rational preventive war; (4) rational miscalculation due to lack of information; and (5) rational miscalculation or disagreement about relative power."[131] While attacking space systems might seem irrational from a space sanctuary perspective, the justifications listed above apply equally across all domains, and space is likely to be included in any future conflict. Senior military officials, as well as many scholars, believe that war in space is looming and according to Jervis, "if the prophecy of hostility is

[128] Zhao, T., and Bin, L. (2017)
[129] Arbatov, A., Dvorkin, V. and Topychkanov, P. (2017)
[130] Fearon, J. (1994), 578.
[131] Fearon, J. (1995), 381.

thoroughly self-fulfilling, the belief that there is a high degree of real conflict will create a conflict that is no longer illusory."[132]

The logic for why states would attack NC3 space systems, specifically, can be addressed in looking at what military objectives would be supported through these attacks. Since the dawn of warfare, gaining the high ground to scout and observe enemy positions and coordinate friendly forces has been a top priority. The NTM ISR satellites that are part of the U.S. NC3 architecture are the most exquisite and capable remote sensing platforms ever created. Not only are they used to monitor strategic nuclear capabilities, but they are also used to support tactical military operations, and everything in between. Information dominance cannot be achieved without denying or degrading these capabilities. However, there has been a massive proliferation of commercial remote sensing platforms over the last 10 years, with the U.S. government as a heavy consumer.[133] The number of systems that would need to be attacked to limit an opponent's ability to monitor actions and achieve information dominance has become prohibitive to all but the most committed attacker.[134] Even with increased use of commercial imagery, NTM ISR systems are the primary method of verifying arms and providing indications and warnings (I&W) of impending launches, so attacks against these systems could be assumed to have a strategic intent, and could result in significant escalation. This is why these systems have been protected in arms agreements and treaties over the last 50 years.

---

[132] Jervis, R. (1976), 77.
[133] Strout, N. (2020); Barnes, J. (2021); National Geospatial-Intelligence Agency (2020); Sadat, M. and Sinclair, M. (2021)
[134] There are now hundreds of remote sensing platforms on orbit that would need to be destroyed to completely blind an adversary. This is in addition to the millions of sensors on cameras/phones/drones and other terrestrial platforms that could be accessed. Large scale military operations no longer have the benefit of unfolding in total secrecy.

Equally important to militaries is the ability to communicate, and information dominance cannot be achieved without limiting an adversary's ability to communicate with dispersed forces. SATCOM systems enable global communications and support data feeds and operations for manned and unmanned platforms. The demand for SATCOM has risen exponentially since the employment of unmanned aircraft (which are controlled remotely over SATCOM links), and as a result, the commercial market in this sector has exploded as well. During the wars in Iraq and Afghanistan, the majority of the U.S.' SATCOM was provided by commercial systems.[135] The protected SATCOM systems that are part of the NC3 architecture do support tactical operations, but again the primary systems employed today are commercial and wideband military satellites. Attacks against protected SATCOM are unlikely to affect tactical capabilities in a meaningful way and instead would send a strong message about adversary intent. These are the systems that nuclear launch messages would flow through and that national command authorities would use to communicate in a degraded nuclear environment, so attacks against these systems would be expected to have severe consequences.

Most critical to the NC3 architecture are missile warning systems. The satellites and RADARs that are part of the missile warning architecture are essential for early warning of strategic launches and enable both missile defense and retaliatory strikes. Unlike ISR and SATCOM, there are no commercial alternatives in the missile warning arena. ISR satellites have limited persistence and revisit times over targets, so adversaries do not even necessarily need to attack these systems to conceal limited operations if they move quickly enough. They can utilize blackout periods that are easily predicted by

[135] From 2000-2011, the DoD's reliance on commercial SATCOM rose over 800 percent and constituted about $1B in spending. Government Accountability Office (2015)

observing orbits or weather conditions to conceal their operations.[136] The same is not true for missile warning systems which provide persistent global coverage. Adversaries cannot hide missile launches or similar attacks that generate infrared signatures, so the only way to conceal those actions would be to attack missile warning systems.[137] This is why it is believed these systems are likely targets for future conflicts. There is a breakdown in logic here that must be accepted, because strategic/nuclear disentangled missile warning satellites would still be able to detect tactical events, so an adversary would need to disable these systems as well. However, even with accepting the argument for disentanglement, the lack of commercial alternatives combined with the vital importance of these systems for early warning and missile defense makes attacks against them all the more serious. Attacks against missile warning satellites are most likely to be met with the most severe consequences.

Finally, all of these justifications for attacks need to be viewed contextually. A single lasing event against an ISR satellite during a period of relative peace is unlikely to generate the same response as the attack would during a crisis. The same goes for SATCOM jamming, or dazzling missile warning sensors, though the latter would still be a significant act. There is no way a state could credibly threaten a massive response to isolated incidents that do not meaningfully degrade NC3 capabilities in aggregate. These attacks would also not be useful for achieving the objectives discussed above and would

[136] Military forces can use cloud cover or darkness to conceal operations from electro-optical (EO) systems, but synthetic aperture RADAR (SAR) would still be effective. A capable adversary can conduct operations when SAR satellites are not imaging over a target area and EO systems are not able to see, but with the proliferation of these systems commercially, these blackout windows are shortening. Additionally, the proliferation of smart phones and social media all but guarantees imagery will be collected and posted at the ground level nearly instantaneously. The ability to conceal military actions has eroded with the growth in sensors, and this trend will continue.

[137] Weather also affects missile warning systems, but in different ways than EO sensors. Specific details will not be discussed to avoid classification issues.

instead be used to demonstrate capability or resolve, or to communicate a threat. My theory does not claim that all attacks against NC3 systems in any context will be deterred, rather I claim that entangled systems are more likely to deter attacks than disentangled systems, and that attacks against entangled systems will be less severe. I argue states understand that attacks against vital strategic assets, like NC3 space systems, would be met with harsh consequences, and also recognize greater opportunity to attack if systems are disentangled. The discussion that follows provides a foundation for my argument by building from deterrence literature.

2.4.2 Deterrence Theory

Fundamentally, deterrence "means persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks."[138] There is disagreement, however, whether deterrence must be based on military strength alone. Scholars like Patrick Morgan emphasize the importance of military threats, claiming that including other means and ends risks "conflating deterrence with other types of preventive measures" thus making "deterrence equivalent to foreign policy as a whole."[139] Robert Jervis postulates that wars occur when states do not develop the "military strength and credible threats necessary to dissuade others from challenging the status quo."[140] Other scholars allow for a broader view of deterrence, including Mearsheimer, who emphasized that deterrence is "a function of the relationship between the perceived political benefits resulting from military action and a number of nonmilitary as well as military costs and risks."[141] Others argue that deterrence can be

[138] Mearsheimer, J. (1985), 14.
[139] Knopf, J. (2009), 35.
[140] Jervis, R. (1993), 244.
[141] Mearsheimer, J. (1985), 14.

achieved through "possession of coercive capability sufficient and appropriate to hold an adversary's valued assets at risk, and to implement a threatened response to an unwanted action."[142] At their core, all of these statements promote a common principle that Knopf captures quite succinctly: "deterrence boils down to anything that can influence others to not do something based on the expectation of a negative result."[143]

Despite myriad opinions on what mechanisms constitute deterrence, "most specialists have recognized at least two distinct paths to deterrence: punishment and denial."[144] Punishment represents the range of tools a state can use to inflict costs against an attacker. Denial includes measures that reduce the anticipated benefits to be gained by an attack. Both punishment and denial are important to a successful deterrence strategy in space, though my theory primarily engages with punishment, as it is the expectation of a more severe punishment that most plausibly deters attacks through entanglement. Deterrence by punishment relies on at least three principles: first are the tools and capabilities necessary to hold an adversary at risk; second is the credibility of a state's resolve, will, and ability to carry out the threat; finally, credibility and capability must be clearly communicated along with what actions an adversary should avoid and the nature of the response if ignored.[145] The principles of deterrence mentioned above are not specific to a particular domain or state. These principles apply equally across domains. Deterrence in space relies on punishment and denial, credible threats, and communication just like all other domains. Deterrence strategies are affected by a number of other

[142]Committee on National Security Space Defense and Protection (2016), 38.
[143] Knopf, J. (2009), 41.
[144] Knopf, J. (2009), 38.
[145] Morgan, P (2003); George and Smoke (1974 and 1989); Schelling, T, (1980); Russett, B (1963); Mazarr, M. (2018)

variables, including methods of communication, intelligence, rationality and irrationality, leadership and interpersonal dynamics, experience, and time pressures, among others.[146]

For the first part of the deterrence equation, all of the states that possess NC3 space systems also have robust capabilities to retaliate, so the ability to punish is fairly straightforward. There is little doubt that any of the states that possess NC3 space systems could punish an attacker, though the type and severity of punishment is uncertain. Next is the resolve, will, and ability to carry out the threat, which is where expectations become a little murkier. According to existing policies and our current understanding of motivations, nuclear weapons would only be employed if a state's survival was threatened, if their vital national interests were threatened, or in the event a state they had a cooperative security agreement with was faced with these circumstances.[147]

There is no expectation that a state would use nuclear force in response to minor territorial disputes or infractions. This is one reason the U.S. strategy of "massive retaliation" was not effective. The idea of using nuclear weapons as a threat for every infraction, no matter how trivial is indeed potent, but it just is not credible.[148] Indeed some scholars do not believe that nuclear retaliation in response to attacks against NC3 space systems is credible.[149] However, as will be discussed later in this chapter, both Chinese and Russian scholars acknowledge that nuclear retaliation is possible, and that this is the type of threat of "things getting out of hand" that could prove to be a powerful

[146] Harrison, R, Jackson, D, and Shackleford, C (2009), 5.
[147] Tannenwald, N. (1999); Press, D., Sagan, S. and Valentino, B. (2013); Posen, B. (1997) Office of the Secretary of Defense (2018); Cohen, A. (2010)
[148] George, A. and Smoke, R. (1989), 177.
[149] Klare, M. (2019)

deterrent.[150] Schelling argues that this fear of "explosive escalation" resolves the "problem of credibility" because the consequence of ignoring the possibility of nuclear escalation is so dangerous.[151] Additionally, even if nuclear retaliation is not credible, adversaries expect severe consequences in response to attacks against vital interests of another state, and entanglement bolsters credibility of threats in this regard.

Nuclear retaliation is a huge step to take and "statesmen have thus far not proven themselves cavalier in taking it."[152] Waltz and others have promoted the value of nuclear weapons in preventing major war and claim that it is still our best source of security and stability in an increasingly unstable world.[153] Third image scholars believe that nuclear weapons are "so scary that the smallest probability of retaliation deters all but the most insane aggressor" and it would be foolish of an adversary to discount the severity of attacks against a state's vital interests.[154] Entanglement makes it impossible for an attacker to avoid targeting nuclear capabilities, even if they have conventional objectives, which keeps nuclear retaliation on the table, in addition to other severe punishments. Disentanglement creates a division between nuclear and non-nuclear, vital and non-vital space systems, and in doing so weakens deterrence. According to Solingen, "nuclear weapons are considered to be well suited to secure survival by generating caution, rough equality, and clarity of relative power."[155] The caution mentioned here is what is at play in my theory of deterrence through entanglement.

[150] Schelling, T. (1966), 97.
[151] Schelling, T. (1966), 97-98.
[152] Posen, B. (1991), 197.
[153] Waltz, K. (2009)
[154] Posen, B. (1991), 209.
[155] Solingen, E. (2007), 24.

Even if we accept that threats of severe retaliation are credible, the threats cannot be effective if they are not communicated. The U.S., Russia, and China have all acknowledged their willingness and ability to use space weapons, but none of these states have established escalation thresholds or provided specific details about what type of response might be expected for attacks against space systems. The existing doctrines of both the U.S. and Russia threaten nuclear retaliation as a potential consequence of attacks against NC3 systems. The 2018 Nuclear Posture Review says that the U.S. could retaliate with nuclear weapons in response to attacks on "U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities."[156] Russian doctrine allows for the use of nuclear weapons in response to non-nuclear attacks "when the state's existence is put under threat," though it is unclear if this is "applicable to responding to strikes against space-based information and communication systems."[157]

Whether or not states would actually respond to conventional attacks against NC3 systems with nuclear force is a source of debate, and there are no historical cases to support either side.[158] We do not yet know how states would perceive attacks in space and how they would respond. Some Chinese scholars do not view attacks against NC3 space systems as constituting a strategic threat, so the threat of nuclear retaliation might not be credible from their perspective.[159] Some Russian scholars on the other hand acknowledge that attacks against NC3 systems could immediately escalate a conflict into a nuclear exchange.[160] Despite the differences in perceptions, it is more likely that

[156] Office of the Secretary of Defense (2018), 21.
[157] Arbatov, A., Dvorkin, V. and Topychkanov, P. (2017), 37.
[158] Kroenig, M., & Massa, M. J. (2021), 3.
[159] Zhao, T., & Bin, L. (2017)
[160] Arbatov, A., Dvorkin, V. and Topychkanov, P. (2017), 37.

adversaries would find threats of significant retaliation and escalation credible when a state's vital interests are threatened, and that is more likely to be the case when NC3 systems are entangled.

It is important to consider that even if the elements above are incorporated into a deterrence strategy, deterrence could still fail. According to George and Smoke, a credible threat alone is not sufficient to deter attacks, rather it is a combination of "credibility and potency of deterrence threat" that ultimately achieves deterrence.[161] I argue that both credibility and potency of threat are increased when nuclear capabilities are involved, as these are vital assets to the states that possess them. Deterrence is a coercive strategy, not a control strategy, so ultimately the would-be attacker's vote counts most. Deterrence only succeeds when a challenger chooses to be deterred, because it is the motivation of the challenger that ultimately determines whether or not an attack occurs. According to Patrick Morgan, challenger motivation is the most important factor in determining whether a deterrence strategy succeeds or fails.[162] With this in mind, states should consider what factors are most able to alter a challenger's motivation when designing deterrence strategies and credible and potent threats. The threat of severe and potentially nuclear retaliation could be very effective as both a credible and potent threat.

2.4.2 Challenges of Deterrence in Space

In addition to the issues listed above, a critical factor for states to consider with deterrence is the ability to attribute attacks. States must be able to attribute attacks, otherwise there can be no credible threat of retaliation. Attribution is extremely

[161] George, A. and Smoke, R. (1989), 177.
[162] Morgan, P. (2003), 164.

complicated in space in general, but particularly so if cyber weapons are used.[163] Gartzke and Lindsay point out that there is a "large and diverse literature, with most authors concluding that deterrence is undermined by difficulties in assigning responsibility for ambiguous attacks."[164] Additionally, even if attribution is possible, it can be extremely challenging to determine intent. Space is an "electro-magnetically active and physically harsh environment" and unintentional interference and anomalies caused by the space environment are common occurrences.[165] Solar charged particles can penetrate spacecraft and cause reboots and other anomalies. Debris that is too small to be tracked can inflict significant damage to a spacecraft. Friendly-force jamming both in space and on the ground is also a common problem. As a result, attribution in the space domain requires sophisticated and robust SSA, intelligence, and geolocation capabilities and investment in SSA is foundational to space deterrence strategies.[166] Harrison et al. make the case that the U.S. "may want to demonstrate that the U.S. edge in attribution (based on its substantial investment in space surveillance and space situational awareness capabilities) provides an asymmetric advantage that could permit escalation dominance."[167]

Even with accurate SSA, the space environment will always be harsh and inhospitable. This could be particularly dangerous if an anomaly occurred during a period of heightened tensions. The difficulty of attribution in space is one of the factors that leads scholars like Acton to believe inadvertent escalation could be an issue in this case.[168] If a system malfunctioned during a crisis, a state could assume the malfunction

[163] Johnson-Freese, J. (2017), 89.
[164] Gartzke, E., & Lindsay, J. (2015), 321.
[165] Harrison, R., Jackson, D., and Shackleford, C. (2009), 14.
[166] Johnson-Freese, J. (2017), 91; Harrison, T. et al. (2017), 31; Klein, J. (2016). Committee on National Security Space Defense and Protection
[167] Harrison, T., et al. (2017), 31.
[168] Acton, J. (2018)

was the result of hostile action, instead of the result of the space environment.[169] With that said, this is not a sufficient reason to jettison entanglement, rather it is another argument to improve SSA capabilities and ensure attribution is possible, whatever the mechanism of malfunction. The challenge of attribution is one of the factors that scholars believe makes deterrence in space more complicated than deterrence in other areas, like nuclear deterrence, though the same issue exists in the cyber domain.[170]

However, there are similarities between nuclear deterrence and deterrence in space. Both domains emerged with competition between the same two powers (U.S. and Soviet Union/Russia) and utilize many of the same systems. The first satellite launch vehicles were ICBMs, many of the first satellites on orbit were used for intelligence collection and arms verification, and NC3 architectures then and now heavily integrate space systems.[171] Specific protections for NTM satellites were also included in arms treaties during the Cold War and continue to be observed by both parties.[172] Both nuclear weapons and space capabilities are considered to be vital national interests as well. All of these factors should lead space to be viewed in the strategic context it deserves. However, despite commonalities between nuclear deterrence and deterrence in the space domain, researchers at the Center for Strategic and International Studies (CSIS) contend that "in the second space age…space has come to be seen as a separate domain with different characteristics and escalation dynamics"[173]

---

[169] Zhao, T., & Bin, L. (2017)
[170] Harrison, T., et al. (2017), 42-44.
[171] Harrison, T., et al. (2017), 24-30.
[172] During the Cold War, protections for NC3 space systems were included in arms reduction and limitation treaties, as well as the ABM treaty. These same protections were also included in New START, which the U.S. and Russia have agreed to extend through February 2026. U.S. Department of State (2022).
[173] Harrison, T., et al. (2017), 24-30.

Despite the lack of space warfare historically, many scholars argue that the United States has not developed an adequate space deterrence strategy, and that overall deterrence in space is low.[174] Some go so far as to say "the ability to deter attacks against networks or satellites is so limited that we can reasonably ask whether deterrence still makes sense as an organizing principle for strategy."[175] There is no single weapon system or threat or defensive posture in space that alone can achieve deterrence.[176] Placing skepticism aside, there are a number of measures that most experts agree contribute to deterrence in space. The single most widely referenced mechanism for deterrence in space is resilience.[177] As discussed previously, resilience preserves capabilities in the face of an attack, which allows for greater flexibility in escalation management, and could also contribute to deterrence by making it cost prohibitive or impossible for adversaries to deny capabilities. In addition to resilience, most scholars believe that norms could help deter conflict in space, not only because of the cooperation and lines of communication that would accompany establishing norms, but because threats of retaliation would be more credible if a state could point to an established norm that was violated.[178]

Outside of resilience and norms, there is disagreement on other mechanisms of deterrence in space. The classical deterrence mechanism of punishment, which is the bedrock of nuclear deterrence, is challenging in space for a few reasons. To begin with, the U.S. is far more dependent on space militarily, economically, and industrially than

[174] Mallory, K. (2018), 8; Harrison, T. et al. (2017), 30-31. Johnson-Frease, J. (2017)
[175] Lewis, J. (2013), 67.
[176] Morgan, F. (2010), 37.
[177] Mallory, K. (2018), 8; Harrison, T. et al. (2017), 30-31. Johnson-Freese, J. (2017); Klein, J. (2006 and 2016); Harrison, R. et al. (2009); Dawson, L. (2018); Triezenberg, B. (2017); Morgan, F. et al. (2018); Finch and Steene (2011); Office of the Assistant Secretary of Defense for Homeland Defense and Global Security. (2015).
[178] Obama, B. (2010); Johnson, K. (2020); Johnson-Freese, J. (2017); Harrison, R. et al. (2009); Morgan, F. (2010); Moltz, J. (2014)

any other state, so threats to punish or retaliate with attacks against space systems "probably lack sufficient potency."[179] Additionally, kinetic attacks in space could generate debris that affects all space actors for thousands of years, and again the U.S. stands to lose the most in this scenario.[180] Finally, threatening to use space weapons could reveal capabilities that adversaries could develop countermeasures for. Like cyberspace, space weapons are probably "better used than threatened."[181] However, as Knopf observed, nothing "inherently limits deterrence to retaliation in kind" and nothing demands that threats be in the same domain as the targets.[182] Punishment for attacks in space can be threatened in other domains, and this is exactly what the U.S.' flexible response strategy promotes.[183] With that in mind, nearly all literature on space deterrence advocates for a layered, cross-domain deterrence strategy.[184] It is still possible to make potent and credible threats for attacks against space systems by threatening to respond in other domains.

The final complication with deterrence in space that I will cover is distinguishability. Challenges with distinguishability can exacerbate the orbital security dilemma and complicate assessments of the offense-defense balance. Glaser and Kaufman believe this challenge is overstated and go as far as to say "whether or not particular weapons are distinguishable has no effect on our ability to calculate the

[179] Morgan, F. (2010), 26-27.
[180] The U.S. military is dependent on space-based capabilities, but the global economy is increasingly space-based as well. GPS, for example, is responsible for about $1B per day in economic impact in the U.S. Skillings, J. (2020)
[181] Gartzke, E., and Lindsay, J. (2017), 37.
[182] Knopf, J. (2009), 41.
[183] Trump, D. (2018); Office of the Secretary of Defense (2018), 23-24, 32, 35, 40.
[184] Johnson-Freese, J. (2017), 87-88; Harrison, R. et al. (2009), 15; Manor, M. (2009), 40; Morgan, F. (2010), 37; Finch and Steene (2011), 13; Committee on National Security Space Defense and Protection. (2016), 26; Mallory (2018), 20-21; Triezenberg, B. (2017); MacDonald, B. (2013); Lewis, J. (2013)

offense-defense balance." [185] Despite this assertion, lack of distinguishability and the rise of dual-use/entangled systems complicates a state's ability to assess the intentions of other states, leaving far more room for misperception. Assessing offense and defense dominance and identifying weapons in space is extremely difficult because most space systems can be used for offensive, defensive, and peaceful purposes, and even clearly offensive systems could be deployed with defensive intentions.[186] Most space systems are inherently capable of offensive actions, even if not specifically designed for that purpose.[187] For example, a commercial satellite command and control (C2) antenna could also be used to jam military satellite transponders; a missile defense interceptor could be used to shoot down launch vehicles or satellites; and launch vehicles could also be used as ASATs. There are dozens of possible hostile uses of technologies that are inherent in peaceful and routine space operations. The inability to distinguish space weapons makes attempts to regulate or prohibit their development nearly impossible and makes deterring attacks all the more important.

2.4.3 Assessing Deterrence in Space

There have been efforts to test space deterrence in experimental settings previously and the CSIS and Secure World Foundation (SWF) space wargaming scenarios conducted in 2016 serve as the basis for my own wargaming scenarios.[188] One of the more interesting revelations from these scenarios was the reluctance to conduct kinetic attacks in space. The authors did not use the word "taboo," but in the scenarios

[185] Glaser, C. and Kaufman, C. (1998), 14.
[186] Klein, J. (2006), 141.
[187] Wright, D., Grego, L., and Gronlund, L. (2005), 10; Johnson-Freese, J. (2017), 90.
[188] Other experimental research for space deterrence has used a game-theoretical approach to determine likely decisions by adversaries, see Triezenberg, B. (2017) and Morgan, F. et al. (2018)

only one kinetic attack was conducted against space systems, despite a willingness to conduct kinetic attacks in other domains. The authors attributed this reluctance to "the fact that most of the participants were familiar with space and thus aware of the possible consequences of attacking satellites" and that if the scenarios were conducted with "a group of people unfamiliar with space, this reluctance might not be present."[189] Through my research, I observed this by testing the same group of students before taking a space security course and after they had taken the course. According to participants, their willingness to attack space systems in initial scenarios and their reluctance in subsequent scenarios was directly related to their understanding of the role space systems play in modern life and the severe consequences that can occur as a result of attacks against space systems.[190] I also found an overall aversion to kinetic space weapons both in my wargaming scenarios as well as surveys. That said, participants in both the CSIS/SWF scenarios as well as my own still chose to attack space systems, though reversible non-kinetic attacks were favored.

Even more relevant to my research was the reluctance of participants in the CSIS and SWF scenarios to attack NC3 space systems, through any means. Researchers noted that all participants viewed attacks against NC3 space systems as "highly escalatory."[191] They also noted that the entangled nature of these systems made it hard for teams to "distinguish between strategic and tactical space systems" and this uncertainty led to difficulty in managing escalation, which the teams did not find as troubling when

[189] Harrison, T., et al. (2017), 44.
[190] The initial set of wargames conducted with these students featured different variables unrelated to entanglement and were not included in my research. Qualitative feedback from participants suggested that an improved understanding of space made them less likely to support attacks against space systems.
[191] Harrison, T., et al. (2017), 44.

attacking conventional forces.[192] Because entanglement was not tested as a variable in these scenarios, the findings do not answer my questions about whether or not entanglement deterred attacks or if disentanglement would've made attacks more likely, but the findings do at least lend credence to my belief that adversaries understand the very significant risks associated with attacking NC3 systems. Adversaries might not believe that nuclear retaliation is credible for attacks against NC3 space systems, but they do appear to understand that there will be a significant escalation which will also be difficult to control. These perceptions should deter attacks, which is what I test.

2.4.4 Dependent Variable (DV): Deterrence

My dependent variable is deterrence, which is operationalized as the likelihood of NC3 space systems to be attacked and is measured using attacks on space systems as a proxy. I define an attack against a space system as *an intentional act by an adversary to degrade, disrupt, deny, or destroy a space capability.* This includes attacks against not only space-based systems, but also the terrestrial command and control infrastructure and space-ground link segments that support the missions. Attacks can be kinetic or non-kinetic, temporary or permanent, reversible or non; an attack is an intentional decision to inflict harm.

Attacks on space systems indicate a failure of deterrence at some level which is why they serve as a proxy for my dependent variable; though for my research the types of attacks conducted are as important as whether attacks occurred. The use of non-kinetic, non-physical, temporary attacks could still signal that deterrence was effective in preventing more lethal attacks. For example, an actor might choose a temporary jamming

[192] Harrison, T., et al. (2017), 44.

attack against a communications satellite instead of a kinetic anti-satellite (ASAT) attack against that satellite because they fear a severe retaliation in the latter scenario. So, even though they chose to conduct an attack, they were deterred from launching a kinetic attack against an NC3 space system. If the DV was measured dichotomously, this granularity would be absent in analysis.

Therefore, instead of measuring attacks only as a dichotomous variable, I also code attacks with a severity score which is based on research done by the RAND Corporation on behalf of Air Force Space Command.[193] Attacks are grouped into four categories based on the severity and expected escalation risk for each type of attack, and are given a multiplier based on category, with kinetic permanent attacks (category/multiplier 4) on the high end of the spectrum and localized non-kinetic temporary attacks (category/multiplier 1) on the low end. Non-kinetic permanent attacks are category/multiplier 3 and non-kinetic temporary attacks are category/multiplier 2. In addition to the quantitative analysis of attacks, I also use qualitative data provided by participants to assess the reasoning and justifications for attacks.

My theory addresses attacks against NC3 space systems, so measuring attacks against those systems is most impactful for testing my hypotheses. However, because participants in the wargaming scenarios are given the option to conduct a broad range of operations to meet their objectives, I am also able to observe what other space systems might be attractive targets, and why. Giving participants the option to conduct a wide range of attacks, both in space and terrestrially was necessary for realism of the wargaming scenarios and to not draw too much attention to the variables being tested.

[193] The RAND Corporation's escalation risk matrix as well as details about coding attacks are found in the research design chapter of the dissertation, Chapter 3.

For example, a state that wanted to conduct an attack to signal resolve or demonstrate a capability might be deterred from attacking an NC3 system but might not be deterred from attacking a commercial system. If the wargaming participants were only asked to consider attacks against NC3 space systems, my findings would not be as complete. The qualitative analysis of participant feedback allows me to better understand motivations for attacking or not attacking a wide array of space systems that would not be possible with a dichotomous treatment of attacks or if only looking at attacks against NC3 space systems.

2.5 Entanglement

Entanglement as a concept in international relations is not new, and entanglement of space systems has garnered more attention in recent years, but the majority of entanglement literature addresses issues of distinguishability and/or the risks of inadvertent escalation. There have been occasional references to the possible deterrent value of entanglement, though no scholars have directly advocated for this position previously, nor have there been empirical studies to examine this hypothesis. The lack of historical cases of escalation as a result of entanglement also makes analysis of the risks of inadvertent escalation very challenging.[194] To further construct my theory of deterrence through entanglement and set the stage for the research that follows, I will cover some of the core principles found in existing entanglement literature, discuss how space system entanglement fits in the broader discussion, address Russian and Chinese perspectives on entanglement, and finally highlight some of the previous works that mention deterrence through entanglement.

[194] Posen, B. (1991), 4; Kroeinig, M. and Massa, M. (2021), 1.

The existing literature on system entanglement is almost entirely focused on inadvertent escalation, which can occur in a variety of ways, but is usually based on a conventional attack that either intentionally or unintentionally affects the nuclear capabilities of a targeted state.[195] The prevailing logic of escalation through entanglement is that entangled systems are attractive targets in conventional conflicts, but the dual conventional/nuclear nature of these systems forces the victim state to escalate because they fear a nuclear attack is forthcoming, or because they must retaliate with nuclear means before the capability to do so is further degraded or lost. The latter scenario is referred to as "use it or lose it."[196] According to Posen, the "most dangerous conventional attacks would be those that substantially degraded the basic nuclear retaliatory capability of the victim" and these attacks could "produce strong reactions from the party on the receiving end."[197] These reactions could include nuclear retaliation, especially if tensions were already heightened or if a state had a launch-on-warning doctrine.[198] However, it is exactly this possibility of severe retaliation that should also contribute to deterrence.

Whatever the likelihood of nuclear retaliation, there are a number of arguments for why inadvertent escalation could occur as a result of attacks on entangled NC3 space systems. These assets are extremely vulnerable to attack, they are vital to state security,

[195] There are a number of works that discuss entanglement and how it contributes to escalation, here are some that are most relevant to my research: Posen, B. (1991); Pollack, J. (2009); Cunningham, F. and Fravel, M. (2015); Rovner, J. (2017); Zhao, T. and Bin, L. (2017); Arbatov, A., Dvorkin, V., and Topychkanov, P. (2017); Tannenwald, N. and Acton, J. (2018); Acton, J. (2018, 2020).
[196] Rovner, J. (2017), 702.
[197] Posen, B. (1991), 1-3.
[198] Launch-on-warning is a doctrine for nuclear retaliation used by Russia. If an attack against vital interests or the homeland is detected and confirmed by additional sensors, then sufficient justification for nuclear retaliation exists. This differs from the launch-on-attack doctrine of the U.S. and the assured retaliation doctrine of China.

they are complex, and they are attractive targets in conventional conflicts.[199] The willingness of potential adversaries to target NC3 space systems in conventional attacks is generally accepted in academic and military circles, and Acton makes the case that the systems are now so complex that an adversary could accidentally (or incidentally) harm them.[200] NC3 systems are "core security assets" and if attacked could leave states unsure of the actions and intentions of their adversaries, which is likely to be a challenge already because of the fog of war.[201] The fog of war could also cause states to misperceive system malfunctions as attacks and escalate a conflict.[202] Ultimately, if a state's vital interests (NC3 space systems) are attacked, the retaliation is likely to be significant, and could go beyond what either party intended, hence the fear of inadvertent escalation.

2.5.1 Russian Perspectives on Entanglement

The U.S. is not the only state with NC3 space systems and concerns about entanglement. Russian scholars have addressed entanglement and escalation to some degree and many of their beliefs echo U.S. concerns. According to Russian space security scholars, "the biggest threat of entanglement would come from the use, during a local or large-scale conventional war, of anti-satellite weapons equipped with non-nuclear warheads against satellites that are a crucial part of the opponent's strategic C3I system."[203] Despite recognizing the risks of significant escalation, Russian military plans include the use of ASATs against NC3 systems because they recognize the important role

[199] Posen, B. (1991); Zhao, T. and Bin, L. (2017); Arbatov, A., Dvorkin, V., and Topychkanov, P. (2017); Tannenwald, N. and Acton, J. (2018); Acton, J. (2018, 2020).
[200] Acton, J. (2018).
[201] Posen, B. (1991), 20-22,
[202] Zhao, T. and Bin, L. (2017), 61; Acton, J. (2018)
[203] Arbatov, A., Dvorkin, V., and Topychkanov, P. (2017), 32. C3I stands for Command, Control, Communication, and Intelligence (or Information). The use of NC3 and C3I are mostly interchangeable, though NC3 specifically identifies systems that are part of the nuclear architecture.

these systems play in Western military operations and power projection and view space systems as "extremely attractive targets."[204] One of Russia's top security concerns is a long-range conventional attack by the U.S. or NATO, but such an attack would depend on vulnerable NC3 space systems, which Russia sees as a vulnerability they "cannot fail to take advantage of."[205] Essentially, Russia views U.S. NC3 space systems as a key vulnerability that could be attacked to reduce the chances of a successful NATO attack against the Russian homeland, but they also recognize the escalation that would occur as a result.

Despite the apparent willingness to target space systems, Russia is aware of the severe consequences these attacks against entangled systems could generate, both for themselves and for the U.S. According to Russian scholars, destruction of NC3 space systems "would threaten to immediately escalate a war to the nuclear level."[206] This might be particularly true for U.S. attacks against Russian space systems because of Russia's launch-on-warning posture. Attacks against Russian missile warning satellites could be viewed as an indication that the U.S. and NATO intended to conduct a counterforce strike against Russia and the Russian government might decide to launch ICBMs to assure their ability to retaliate. However, "Moscow believes that the United States understands all the consequences of attacking this kind of Russian satellite, and that the United States would react in exactly the same way to an analogous attack on its own early-warning satellites."[207] This is a critical point. Russia is well aware of the vital role NC3 space systems play both for their own defense and for the U.S. and expect that

[204] Buzhinsky, E. (2009)
[205] Arbatov, A., Dvorkin, V., and Topychkanov, P. (2017), 36.
[206] Arbatov, A., Dvorkin, V., and Topychkanov, P. (2017), 38.
[207] Arbatov, A., Dvorkin, V., and Topychkanov, P. (2017), 38-39.

attacks against these systems would incur harsh consequences. The U.S. and Russia have many comparable NC3 space capabilities from a technical standpoint and have agreed to protect these systems historically, so it makes sense that scholars and military leaders in both countries have similar views on entanglement and escalation. China on the other hand, does not appear to have a cohesive viewpoint on entanglement and escalation.

2.5.2 Chinese Perspectives on Entanglement

According to Chinese military scholars Zhao and Bin, the issue of entanglement has rarely been a focus for the Chinese government or military leaders, and when it is considered, the implications of attacks against entangled systems are not always consistent with U.S. views.[208] The authors agree that Beijing could be tempted to conduct attacks against U.S. NC3 space systems in a regional conventional conflict, like the invasion of Taiwan, but state that some Chinese military leaders believe these attacks would "clearly constitute a tactical military operation with the limited objective of undermining U.S. theater missile defense capabilities in the region."[209] Additionally, some Chinese experts "neglect the possibility that the United States might interpret such strikes as preparations for the first use of nuclear weapons" and even go so far as to claim that "anti-satellite weapons could not, by definition, provoke a nuclear attack."[210] This difference in perception and expectation is what Zhao and Bin look to as the source of potential inadvertent escalation in a U.S.-China conflict, and something I also observed in the elite surveys I conducted. Even when Chinese experts recognize the risks of escalation through entanglement, there is no consensus on how best to respond. In the

[208] Zhao, T. and Bin, L. (2017)
[209] Zhao, T. and Bin, L. (2017), 52.
[210] Zhao, T. and Bin, L. (2017), 52, 64.

Chinese view, it is the U.S.' responsibility to reduce the risks, because it is the U.S. policy of launch-under-attack that is to blame for the risks.[211]

There is also no consensus amongst Chinese leaders on how entanglement of NC3 systems should be handled. In one camp are those that view entanglement as a negligible concern and believe ASATs are useful for military operations and should not be perceived as constituting a nuclear threat. In the other camp are those that recognize the possible deterrence value of entanglement and believe that disentanglement (or decoupling in their words) "might be exploited by potential enemies, which could feel more comfortable with conducting strikes against Chinese conventional capabilities."[212] The second camp seems to have prevailed thus far from a policy standpoint. Although China did not intentionally entangle systems as a mechanism of deterrence, China is now "reluctant to increase its vulnerability by embarking on a process of separation."[213] This finding is particularly relevant to my research, as the U.S. has embarked on a process of separation already, which like the Chinese, I argue increases vulnerability. It is unclear whether Chinese experts believe entanglement deters Chinese attacks against U.S. systems, but they do appear to believe entanglement will deter U.S. attacks against Chinese systems. This underappreciated possibility of deterrence through entanglement is the basis for my research.

2.5.3 Entanglement and Deterrence

Like China, Russia has not intentionally entangled systems for deterrence, but their NC3 systems are also entangled, and this could be an ancillary benefit. According to

[211] Zhao, T. and Bin, L. (2017), 57.
[212] Zhao, T. and Bin, L. (2017), 68.
[213] Zhao, T. and Bin, L. (2017), 68.

Acton, "the co-location of nuclear and general-purpose forces in the Soviet Union and now in Russia was and is prompted by economic and administrative considerations, not by the strategic goal of trying to deter U.S. non-nuclear strikes against Russian general-purpose forces through the threat of nuclear escalation."[214] Even as a leading voice in the inadvertent escalation literature, Acton recognizes that there could be deterrence value in entanglement and he advocates for governments to study these possible benefits.[215] This research attempts to fill the gap that has been so far neglected by governments. In another recently-published work, Kroenig and Massa state that "countries may intentionally pursue deterrence through entanglement" because "leaders might conclude that attacking dual-use capabilities is too risky."[216] They go on to say that leaders "might voluntarily refrain from attacking certain targets in order to avoid the escalatory risks" and "adversaries could become more cautious around dual-use systems in crises in a way that contributes to stability."[217]

Other security scholars have also alluded to the possibility of deterrence through entanglement. In writing about Chinese nuclear and conventional force "comingling," Cunningham and Fravel say that increasing the degree of comingling indicates "China's efforts to intentionally increase the risk of nuclear escalation in the event of a U.S. conventional strike on its missile bases."[218] In this case, the authors are not specifically talking about NC3 space system entanglement, rather the positioning of nuclear and conventional forces and equipment together, but the logic still applies. Posen also did not

[214] Acton, J. (2017), 2.
[215] Acton, J. (2018), 92-93.
[216] Kroenig, M., and Massa, M. (2021), 11.
[217] Kroenig, M., and Massa, M. (2021), 11.
[218] Cunningham, F. and Fravel, M. (2015), 45.

specifically address deterrence through entanglement, but he did promote the powerful deterrence effect of nuclear retaliation, which he said could be a prospect that "deters even ambitious powers from most challenges."[219] If a nation's vital NC3 infrastructure is threatened, attackers must contend with the possibility of a devastating nuclear response. This threat of severe retaliation and uncontrolled escalation is the mechanism that should deter adversaries from attacking NC3 systems.

Conversely, deterrence could be weakened if a state prioritized conventional forces as a safeguard, which is what disentanglement accomplishes. Building substantial conventional capability can "postpone the prospect of nuclear escalation indefinitely" which could ultimately make conventional war more likely.[220] Disentanglement, while trying to avoid nuclear escalation, could actually give states greater incentive to attack due to a perceived ability to avoid the most severe consequences. Entanglement on the other hand puts a state's vital interests at stake and "vital issues are better deterred if the adversary fears rapid nuclear escalation as a consequence of mutual offensive incentives."[221]

2.5.4 Challenging Inadvertent Escalation as a Result of Entanglement

The primary argument against entanglement of NC3 space systems has not focused on deterrence at all; much of the entanglement debate centers around inadvertent escalation. In their recently published work, Kroenig and Massa call into question the logic of inadvertent escalation as a result of entanglement. With no historical cases to support escalation through entanglement, previous scholarship has been based on

[219] Posen, B. (1991), 204.
[220] Posen, B. (1991), 205, 210.
[221] Posen, B. (1991), 207.

hypothesized scenarios of how escalation could occur. According to Kroenig and Massa, these hypothesized scenarios are "logically inconsistent, lack strategic empathy, and do not account for operational obstacles to nuclear preemption."[222] The authors use analysis of India and Pakistan to demonstrate that conflicts have occurred between nuclear states, and these conflicts have involved nuclear/conventional capable systems, yet inadvertent escalation has not occurred as a result. This is yet another reason to question the decision to disentangle NC3 space systems. Besides deterrence, Kroenig and Massa argue that the fundamental logic underlying escalation through entanglement could be flawed. That alone would be reason to question the decision to disentangle systems, but this claim is also untested in the space domain.

2.5.5 Other Types of Space System Entanglement

To close out the discussion of entanglement, it is useful to note that other types of entanglement in the space domain have been brought forward in existing literature. I will not go into great detail as these entanglement cases are not directly tested in my research, but the logic behind these claims applies to the nuclear/conventional entanglement I investigate. Deterrence rests on the perception that consequences of an action will be higher than the expected benefit of that action, and this is assumed to be true for the cases presented below. Each of these types of space system entanglement increase the costs of an attack for a potential adversary. The same can be said for the nuclear/conventional system entanglement I investigate, so the same deterrence logic should apply.

[222] Kroenig, M., and Massa, M. (2021), 2.

Table 2 - Types of space system entanglement and impact on deterrence

Type of Entanglement	Examples	How it Deters
Military - Civilian[223] (Military Operated)	GPS, SSA, human spaceflight	Systems that perform both military and civilian functions could cause harm to civilian populations if attacked (including within the attacking state), which could dramatically affect public opinion and could involve a greater number of states in the conflict than was intended originally.
Military - Commercial[224] (Commercial Operated)	Commercial SATCOM, ISR, launch	Attacks against commercial systems could invite consequences from all parties who utilize the system, across multiple states.
Military - Foreign[225] (Foreign Operated)	Foreign government SATCOM, ISR, weather, SSA, etc.	Attacks against third party foreign systems could invite retaliation from parties that otherwise would have been neutral.

2.5.6 Independent Variable: Entanglement

The independent variable I test in the experimental portions of this research is NC3 space system entanglement. For the purposes of my research, this variable can take three forms: systems are either entangled, disentangled, or entanglement status is unknown. In reality, varying levels of entanglement could be implemented within a state's space architecture but testing the infinite range of possible configurations is not feasible within the scope of this research. For example, a state could choose to disentangle ISR and SATCOM systems, while leaving missile warning systems entangled, or leave a portion of systems entangled. For my research, I assume all of the state's NC3 space systems are either entangled, disentangled, or unknown. Also in the

[223] Harrison, T. et al. (2009); Manor, M. and Neuman, K. (2009)
[224] Harrison, T. et al. (2009)
[225] Morgan, F. (2010); Harrison, T. et al. (2009)

real world, states should be aware of the entanglement status of systems through their intelligence collection capabilities as well as publicly available information about the systems released by the states that operate them. This information can be accessed through launch manifests, spacecraft registration, news releases, and a host of other unclassified and classified sources. However, I use unknown entanglement status to establish a baseline for how states might behave and what attacks might occur with no knowledge of entanglement. This control group allows me to better understand if entanglement actually affects outcomes. In the scenarios and surveys, I provide short statements about the entanglement status of participants' own systems as well as their adversary's NC3 systems. Additionally, I provide a statement about how their state's capabilities are affected should these systems be attacked.

2.6 Arguments for Disentanglement

Even if the possible deterrence value of entanglement is accepted, the argument can be made that disentanglement is a safer strategy because it could provide a state more options for managing escalation and provide more "room to be cheated."[226] According to Jervis, states that "cannot be destroyed by a surprise attack can more easily trust others and need not act at the first, and ambiguous, sign of menace."[227] Attacks against disentangled conventional systems could be more easily absorbed than attacks against entangled NC3 systems, and that could provide greater flexibility with managing escalation. However, my research focuses on deterring attacks rather than managing escalation following attacks. It is logical to assume that disentanglement allows for greater flexibility in escalation management following attacks, but this is also an

[226] Jervis, R. (1978), 198.
[227] Jervis, R. (1978), 172, 174.

unproven hypothetical in the space domain. It is also possible that attacks against disentangled conventional systems could lead to inadvertent and uncontrolled escalation.[228] Entangled systems could also provide more flexibility for escalation management because victim states would theoretically have more justification for a wider range of response options. They could choose massive retaliation by citing impacts to NC3 or they could choose a lower level of retaliation claiming that they understood the intent was not to disrupt NC3. Instead of relying on entanglement or disentanglement alone to preserve more rungs on the escalation ladder, other measures like resilience could be enacted, which could provide more room to be cheated while also keeping systems entangled.

In the argument for disentanglement, the DoD has conflated disentanglement and resilience, which is a big part of the problem with the current strategy. As discussed in Chapter 1, entangled satellite systems could also be made more resilient through many of the same methods used for disentangled systems. NC3 satellites could be dispersed in greater numbers across different orbits, they could be made smaller and harder to attack, they could be reconstituted more quickly, or any number of other options that enhance resilience.[229] None of these measures are mutually exclusive with entanglement. It is very possible to have a resilient architecture that is also entangled, and I would argue that this is actually the best possible scenario. A state could achieve even greater deterrence through a resilient entangled architecture because it would maximize deterrence by

[228] In the space security wargames conducted by CSIS, some participants viewed non-kinetic reversible attacks to be as escalatory as kinetic permanent attacks, so it is not a given that attacks against disentangled systems will be viewed as less escalatory. Harrison, T. et al. (2017), 42.
[229] A good overview of space system resilience can be found in the Space Domain Mission Assurance report from Office of the Assistant Secretary of Defense for Homeland Defense and Global Security (2015); see also Taverney, T. (2011) and Air Force Space Command (2016).

punishment and denial. By implementing both punishment (entanglement) and denial (resilience) mechanisms, it is possible to "operate on both sides of a potential adversary's cost-benefit decision calculus simultaneously."[230]

I do not attempt to address all of the possible mechanisms that could contribute to deterrence in space, nor do I claim my theory of deterrence through entanglement applies beyond NC3 space systems. I present information about resilience in Chapter 1 and above because it is one of the primary justifications the DoD uses to explain why disentanglement is necessary and why it leads to deterrence. My argument accepts the widely shared belief that resilience contributes to deterrence; I differ in that I argue entangled architectures are equally good candidates for resilience. I do not test space system resilience or other space deterrence mechanisms in my research.[231]

The primary competing claim to my theory of deterrence through entanglement is not actually about deterrence, it is about inadvertent escalation. As discussed previously, there are very significant fears about inadvertent escalation as a result of entanglement. However, as Kroenig and Massa argue in their recent brief, the risk of inadvertent escalation has been overstated, there are no historical cases of inadvertent escalation as a result of entanglement, and the logic of inadvertent escalation also lends support to the value of entanglement for deterrence.[232] Potential adversaries must contend with the possibility that escalation could be uncontrolled and much greater than they intended, and this awareness could deter attacks.

---

[230] Morgan, F. (2010), xiv.
[231] There are a number of great works that focus on deterrence broadly in the space domain, and what mechanisms most contribute to deterrence. See: Morgan, F. (2010); Moltz, J. (2008 and 2014); Morgan, F. et al (2008); Manzo, V. (2011); Klein, J. (2006); Johnson-Freese, J. (2017); Harrison, R., Jackson, D. and Shackleford, C. (2009); Lewis, J. (2013); MacDonald, B. (2013); Krepon, M. (2013); Harrison, T. et al. (2017)
[232] Kroenig, M. and Massa, M. (2021)

Finally, it can be argued that regardless of whether or not entanglement is a useful deterrent, it constrains states in their ability to respond to attacks and invites confusion with respect to adversary intent. With disentangled systems, it would be easier for states to understand the intentions of their adversaries. If conventional systems are attacked, the objective is not likely to be to cripple nuclear capabilities, whereas if disentangled nuclear systems are attacked, this would more clearly indicate an imminent nuclear attack. A state might decide that the ability to more easily gauge intent outweighs the possible deterrence value provided by entanglement. A state might also be willing to accept attacks against conventional systems in order to maintain more control over escalation. These tradeoffs will need to be weighed by policy makers, but as of now, they are not armed with any evidence to support the claims on either side.

Ultimately my theory underscores a classic competition in risk taking. Leaving NC3 systems entangled could incur risks of inadvertent escalation. On the other hand, disentanglement could incur the risk of a higher likelihood of attacks. This balance of risk is not unique to the space domain nor is it unique to entanglement. Deterrence theory as a whole "rests on the notion of the manipulation of risk."[233] This case does have very real policy implications, however, and in order for decision makers to adequately weigh and manipulate the potential benefits and risks of entanglement, experimental research must first be conducted to test how these competing beliefs are supported by evidence. As of now, all we have is theory.

[233] Jervis, R. (1979), 310.

2.7 Alternative Explanations

While my theory and research specifically address the effects of entanglement on decision making, it is reasonable to assume that other factors influence decisions to attack NC3 space systems. Some of these alternative explanations will be tested through my research, while others are merely considerations for my research design and data analysis. Some of these considerations are incorporated into my theory already but could be treated as additional independent or conditional variables under a different research design. The first set of considerations fall into a category of adversary awareness. As discussed earlier in this chapter, I assume that potential adversaries that have the capability to attack NC3 space systems also have awareness of system entanglement. With that said, I use an unknown entanglement status treatment not only to set a baseline with which to compare entangled and disentangled responses, but also to address the possible case of adversaries being unaware of entanglement. In addition to awareness of entanglement status, the theory of deterrence through entanglement is predicated upon awareness of policies, threats, and severity of response. I do not vary stated policies or threats in my research design, but it is possible that treating one or both of these areas independently could affect decision making. The choice not to vary these elements of awareness was deliberate and intended to isolate entanglement status as the lone IV to ensure the effects of entanglement on the DV could be observed more clearly.

In addition to *awareness* of policies and threats, deterrence depends on perceptions of *credibility* of threats. If potential adversaries believe threats of severe retaliation in response to attacks against NC3 space systems to be credible, they are more likely to be deterred from attacking these systems. Conversely, if credibility is not

present, deterrence will be weakened. Therefore, perceptions about the credibility of threats could be an alternative explanation for deterrence through entanglement. This seems logical, but it is important to point out that credibility is not independent of my theory. Instead, underlying my theory is an assumption that the threat of severe retaliation in response to attacks against NC3 space systems is perceived by potential attackers as credible. Additionally, I argue that credibility is strengthened or weakened in part by entanglement status. Severe retaliation is more credible when a state's most vital interests are threatened, like NC3 systems. If entangled or disentangled nuclear systems are attacked, a state's vital strategic capabilities are threatened, and the retaliation should be most severe. It would not be as credible to threaten severe or nuclear retaliation in response to attacks against disentangled conventional systems. That said, credibility is in the eye of the decision maker and could vary greatly based on context and individual beliefs. In both the wargames and elite surveys, I assessed perceptions of the credibility of threatening nuclear retaliation in response to attacks against NC3 space systems; the results are covered in the empirical chapters.

In a related vein, decisions to attack NC3 space systems could be significantly affected by expected responses, which is slightly different than credibility. It is possible for a potential attacker to believe threats of severe retaliation to be credible without believing these threats to be likely. If a potential attacker believes retaliation is most likely to be tolerable, they are less likely to be deterred. Like the credibility perceptions, expectations of likely responses are context dependent and could vary by individual. It is likely that retaliation would be less severe for non-kinetic reversible attacks compared to kinetic attacks, but that is not guaranteed. Potential attackers could also expect retaliation

to be proportional, so if they chose to use non-kinetic weapons, they might expect that non-kinetic weapons would be used in response. These perceptions of likely victim response are context and individual dependent, but could help explain why given the same inputs, participants within each treatment respond similarly or differently. Perceptions about types of attacks and likely responses are assessed with both quantitative and qualitative data and are covered in the empirical chapters.

2.8 Summarizing the Theory of Deterrence Through Entanglement

The theory of deterrence through entanglement operates on a few key premises. First, entanglement guarantees that attacks against NC3 space systems, even if intended to achieve limited conventional objectives, will affect the strategic/nuclear capabilities of a targeted state. Potential attackers must confront this fact when deciding whether or not to conduct attacks and must be willing to risk the consequences (punishment) associated with degrading a state's nuclear capabilities. This is also true of disentangled nuclear systems, as attacks against these systems would directly affect the NC3 capabilities of a targeted state as well. Second, because NC3 capabilities are among a state's most vital interests, it is credible to threaten severe and possibly nuclear retaliation in response to attacks against entangled and disentangled nuclear systems. This is the credible threat of severe punishment at the core of deterrence through entanglement. Finally, the theory assumes that potential attackers are aware of entanglement status as well as policies and threats related to attacks against these systems. Without awareness of entanglement or an expectation of severe retaliation, deterrence through entanglement will not be achieved. As discussed in the previous section, potential attackers must also believe severe

retaliation, or consequences reaching a level that outweighs expected benefits, must not only be credible but likely in order to deter attacks.

Under the logic of this theory, disentangled nuclear systems could potentially be the safest from attack as attacks against these systems would be unambiguously intended to affect NC3 capabilities. There are fewer plausible justifications for attacking these systems to achieve limited regional or conventional objectives. However, even though nuclear systems might be safer, disentanglement gives potential attackers another set of targets with lower expected costs for attacks, and that is ultimately what makes attacks in general and specifically against these disentangled conventional systems more likely. An adversary could feel safer attacking disentangled conventional systems due to the ability to leave strategic/nuclear capabilities of the targeted state unaffected. Ultimately, the theory of deterrence through entanglement is a theory of *expected costs* for attacks. From this logic, I form two hypotheses:

H1: Entanglement deters attacks against NC3 space systems.

Attacks against entangled systems affect the vital nuclear capabilities of a targeted state, and as such, severe retaliation is both expected and credible. Deterrence through entanglement is achieved as a result of a potential attacker's expectations of severe punishment. Under this hypothesis, I expect potential attackers to conclude that the risks of severe retaliation outweigh the expected benefits of the attack and therefore there should be fewer attacks against entangled NC3 space systems compared to other entanglement treatments. It is possible and even likely that disentangled nuclear systems would be safest from attack, as these attacks should only be conducted by attackers with nuclear objectives, however, these systems are only half of the disentangled architecture,

so as a whole entangled treatments should see fewer attacks. As discussed in the preceding section, expectations of retaliation are also context dependent, so if/when entangled systems are attacked, I expect attacks to be conducted using less severe means (ex. reversible non-kinetic attacks) compared to other treatments, in an effort to limit the severity of the response.

H2: Disentanglement of NC3 space systems makes attacks against conventional versions of the disentangled systems more likely.

Operating on the other side of the theory's logic, potential attackers should reasonably expect less severe retaliation for attacks against disentangled conventional systems because these attacks would not affect a targeted state's vital NC3 capabilities. Severe retaliation for attacks against disentangled conventional systems is both unlikely and un-credible, so potential attackers should conclude attacks against these systems could be carried out with a lower risk of unacceptable retaliation and escalation. Under this hypothesis, I expect to see a greater number of attacks against disentangled conventional systems compared to entangled systems.

The table below captures the logic of both hypotheses:

Table 3 - Underlying Logic of Theory and Hypotheses

Condition	Impact	Response	Expectation
NC3 systems are entangled[234]	- Attacks will affect vital nuclear capabilities of targeted state - Targeted state could assume nuclear attack is imminent	- Retaliation will be severe, possibly nuclear - Significant uncontrolled or inadvertent escalation likely	- Adversary will be deterred
NC3 systems are disentangled	- Attacks can occur against conventional systems without affecting state's nuclear capabilities	- Retaliation will be in kind, proportionate - Escalation can be incremental and managed	- Adversary will not be deterred - Attacks against conventional systems are more likely

If the hypotheses above are true, the decision of whether or not entanglement or disentanglement should be pursued becomes a question of priorities. If entanglement deters the greatest number of attacks overall, that could make space a safer domain for all operators and minimize the attacks against military spacecraft. However, if the goal is only to deter attacks against nuclear systems, and attacks against conventional systems could be tolerated, then disentanglement might be the favored strategy. Regardless, this is a question for policy makers, but at the very least, entanglement as a variable needs to be tested. My theory of deterrence through entanglement and the analysis that follow this chapter contribute to the scarce literature on this topic and provide the first-ever empirical analysis that treats entanglement as an independent variable. This research is an

[234] This also applies to disentangled nuclear versions of systems.

investigation into perceptions about expected costs and how these perceptions influence the decision to attack or not attack NC3 space systems.

CHAPTER 3. RESEARCH APPROACH

3.1 Methodology

To empirically test my theory of deterrence through entanglement, I utilize two complementary experimental approaches. The first are space security wargaming scenarios utilizing undergraduate and graduate students as well as Reserve Officer Training Corps (ROTC) cadets at the Georgia Institute of Technology. The second method involves survey experiments completed with space security elites as well as a public sample. Wargames are useful for observing human interaction and decision making in a fluid and competitive environment, which can simulate some of the interpersonal and time-factor dynamics at play when these types of decisions are made in the real world. While surveys lack interaction and time pressures, they add value by allowing researchers to control inputs and treatments more precisely and aggregate and analyze data more efficiently. Surveys are also less time consuming and allow for a greater sample size and ability to target elite populations more easily. Taken together, both methods provide sufficient data to test my hypotheses.

Experiments have become a popular research method for political scientists and IR scholars, particularly when investigating topics that are difficult or impossible to observe in the real world or through historical cases.[235] Over the last 20 years, more than 900 experiments have been published in the "big 3 journals in political science" with more than 800 of these experiments involving general public or non-elite samples.[236] The space domain is well suited for experimental research because unlike other domains,

[235] Kertzer, J. and Renshon, J. (2022); Lin-Greenberg, E., Pauly, R., and Schneider, J.
[236] Kertzer, J. and Renshon, J. (2022), 4.

there are no historical cases of space war or hostile kinetic attacks in space that can be analyzed. Therefore, it is impossible to empirically assess the likelihood of attacks against NC3 space systems without taking an experimental approach. Below I will discuss the utility and rationale behind the methods I have selected and address criticisms of using experimental approaches, specifically the use of students as participants in political science research experiments. Details about the design and conduct of the experiments, as well as the data collected, will be covered in the subsequent empirical chapters, Chapter 4 (wargames) and Chapter 5 (surveys).

3.1.1 Space Security Wargames

According to Lin-Greenberg, Pauly, and Schneider, "scholar-generated wargames are best used to answer questions about human decisionmaking, either regarding rare events, or topics where real-world data are difficult to obtain."[237] With no hsitorical cases of war in space and a highly complex and restrictive operating environment, space is a domain well-suited to wargaming. More simply, the experimental research I am conducting cannot be tested in a real-world setting. Wargames provide a telescope through which decision makers can test strategies and observe events that have never before transpired and apply the lessons they learn "before committing blood and treasure."[238] Additionally, the theory I present is ultimately a theory of decision making; specifically the decision of whether to attack space sysems or to be deterred from doing so. Wargames are useful for observing these kinds of crisis decision points because they create an environment with time pressures and human interactions that "induce players to behave in ways that closely mirror their behavior when presented with similar real-world

[237] Lin-Greenberg, E., Pauly, R., and Schneider, J. (2022), 15.
[238] Herman, M., Frost, M., & Kurz, R. (2009), 4-7.

contexts."[239] Wargames are a human endeavor that "revolve around the interplay of human decisions and game events" and "this active and central involvement of human beings is the charactersitic that distinguishes wargames from other types of models and simulations."[240]

In his 1990 book *The Art of Wargaming*, Peter Perla asserts that wargames are intrinsically studies of humans and learning. Perla states that wargames are very useful as exploratory tools because they "can give players, analysts, and other observers and participants new insights, which can lead them to further investigation of the validity and sources of their beliefs."[241] These insights arise as a result of interactions between players that cannot be easily modeled or replicated using other types of research. Additionally, the competitive interactions between players create fluid environments with group decision making that more closely resembles real-world situations than other types of experiments, like surveys. This positive aspect of wargaming is also identified by Lin-Greenberg, Pauly and Schneider who say, "the interactions of players within and across teams that ultimately shape decisions during wargames are important because real-world foreign policy decisions are rarely made by a single individual."[242] This is one of the primary reasons I selected wargames as a research method for evaluating my theory. The decision to attack satellites will not be made by a single individual operating in a vacuum (even if the attacks would occur in the vacuum of space), so wargames are valuable for simulating the group dynamics and crisis pressures that would occur in a real setting.

[239] Lin-Greenberg, E., Pauly, R., and Schneider, J. (2022), 5.
[240] Perla, P. (1990), 30.
[241] Perla, P. (1990), 194.
[242] Lin-Greenberg, E., Pauly, R., and Schneider, J. (2022), 12.

Peter Perla and Ed McGrady also speak to the value of human interaction in their article "Why Wargaming Works." The authors find that one of the most unique and beneficial aspects of wargaming is that players and participants are forced to constantly communicate, interact, and react to the decisions and inputs of other participants. The authors claim that "this creates a conversation among everyone involved in the game, one that creates a unique narrative."[243] The interaction of players and the generation of a unique narrative differs significantly from modeling and simulation, as well as text-based, non-interactive analyses. Pulling from cognitive-neuroscience, the authors find that "the normal narrative disbelief that arises from a reader's inability to act on the information presented in a text narrative is foiled in a game, because the player actually can (and must) act on the narrative information the game presents."[244] This is the reason I did not want to use only survey experiments or other text-based research methods. With wargaming, participants can more easily assume the roles they are being asked to play and I gain valuable data by observing interactions that aren't possible with other methods.

Wargaming has served as an important tool for understanding conflict and decision making in crises for at least the last 300 years. Wargaming was practiced heavily in 18th and 19th century European conflicts and is widely used globally by militaries and policy makers today.[245] Wargaming also has a rich history of challenging existing beliefs and influencing strategy and policy in the U.S. In the book *Wargaming for Leaders*, Herman, Frost, and Kurz provide lessons from wargames they conducted over several decades for the U.S. Government to make some salient points about the importance and

[243] Perla, P. and McGrady, E. (2011), 118.
[244] Perla, P. and McGrady, E. (2011), 121.
[245] Perla, P. (1990), 36-37.

limitations of wargames. They begin the book by extolling the utility of observing possible futures, free from the risk of harm that could be generated by making decisions in the real environment.[246]

The authors recall a wargame in the 1980s that was conducted to test parts of the Strategic Defense Initiative (SDI). The SDI would have used space-based and other defenses to shoot down intercontinental ballistic missiles (ICBMs) launched from the Soviet Union. The idea was initially dismissed as ludicrous under the assumption that SDI would need to be 100% effective to be useful, which would be impossible given the Soviet Union's stockpile of over 15,000 nuclear warheads. Wargaming showed otherwise. Even with defense effectiveness set as low as 15%, the Soviet "red team" players had to assume that every strategic target on their priority list was defended. As a result, the notion that defenses must be perfect eroded.[247] Like SDI, the effects of entanglement and disentanglement cannot be tested in a real-world setting, and in order to challenge commonly held beliefs about entanglement, I need to be able to gather data.

The absence of space warfare historically and the inability to test these concepts in a real-world environment have made wargames a valuable research method for space security experiments. The wargames that informed my own design were conducted by CSIS and the Secure World Foundation in 2016, with the findings published in the report *Escalation and Deterrence in the Second Space Age* in 2017. In order to assess possible outcomes of space conflict, the authors created three distinct space crisis scenarios and conducted tabletop exercises (wargames) with experts from the space community.[248]

[246] Herman, M., Frost, M., and Kurz, R. (2009), 4-7.
[247] Herman, M., Frost, M., and Kurz, R. (2009), 30-34.
[248] Harrison, T., et al. (2017)

Researchers from CSIS conducted another set of experiments in 2020 with elites to assess space system defenses through four realistic crisis scenarios.[249] While extremely informative from a broader space conflict perspective, these wargames did not address entanglement.

Other scholars have taken different approaches to understanding space conflict and deterrence. In her dissertation, Bonnie Triezenberg used a game-theoretic approach infused with prospect theory to assess how sentiments could affect space conflict. Triezenberg builds upon deterrence literature and applies prospect theory to the space domain in an interesting way, namely moving away from the rational actor view of state behavior. This effort succeeds in providing a high-level view of space conflict and deterrence from a game-theory perspective, while also providing some useful policy recommendations.[250] In a similar vein, Forrest Morgan and his colleagues from the RAND Corporation completed a project for the U.S. Air Force in which they used game theory to assess potential adversary tactics against space systems as well as possible defensive actions. Again, however, questions about the utility of deterrence mechanisms, like resilience or entanglement, are not answered.[251] For my own research, I drew from the RAND Corporation's escalation risk matrix to categorize NC3 space system attacks further by severity (escalation risk), beyond the simple count of numbers of attacks.[252]

In addition to the unclassified space security wargames mentioned above, the Department of Defense conducts classified wargames annually. Historically, space was

[249] Harrison, T., Johnson, K., and Young, M. (2021)
[250] Triezenberg, B. (2017)
[251] Morgan, F., et al. (2018)
[252] Both the RAND Corporation's escalation risk matrix as well as my table are presented in the research design section of Chapter 4.

integrated into DoD wargames in a supporting role with the focus on space as a service provider to the rest of the combat capabilities being observed, rather than an important domain for analysis in its own right. That is now changing, however, and more efforts are underway to integrate space as a potential warfighting domain, just as air, land, sea, and now cyber are regarded. [253] The Schriever wargames are one of the DoD's premier mechanisms for evaluating future space conflict scenarios through a strategic lens. Held annually, these wargames bring in senior leaders and participants from around the world and across the DoD to tackle some of the biggest challenges confronting space security.[254] More recently, the Air Force has begun Space Flag exercises, which are held twice a year, and are designed to prepare operators at the tactical level for space warfare. According to Air Force Space Command, which dissolved with the creation of the United States Space Force, "the goal of the exercise is to enable forces to achieve and maintain space superiority in a contested, degraded and operationally limited environment."[255]

While it is useful for the DoD to conduct classified wargames, classification is also a significant limitation. The unclassified reporting following the events is paltry, containing only major themes and generalities; nothing that could be used for rigorous analysis by academia or outside organizations. On one hand, the nature of the scenarios requires classification, as real systems are assessed against real threats. On the other hand, classified and isolated exercises and wargames create a very myopic and military-centric approach to space security challenges. It is possible that the subject of my research has already been investigated and wargamed in classified settings, and if that is

[253] Caffrey Jr., M (2019)
[254] Hill, L. (2019)
[255] Air Force Space Command Public Affairs. (2019)

the case it could be useful to compare findings. However, the military and academia could benefit from greater integration in the space conflict arena, and that is one of the goals of my research moving forward. The table below provides a snapshot of some of the previous space security wargames.

Table 4 - Previous Space Security Wargaming and Experiments

Wargame	Author	Variables	Findings
Defense Against the Dark Arts (2021)	CSIS	Maneuvering NC3 systems, GPS defenses, counterspace weapons, commercial system protection	Need better SDA, norms, thresholds. Cyber attacks were favored and viewed as safer. Proportional attacks in space are not ideal.
Gaming Space (2018)	RAND	Computer-based game-theoretic assessment of space control options	Pursuit of dominant strategies; achieve objectives with acceptable escalation risk and political costs.
Deterring Space War (2017)	Triezenberg (RAND)	Prospect theory approach to game theory analysis of space deterrence	Sentiment/emotions affect outcomes, resiliency and redundancy deter attacks; weapons are needed in limited quantities.
Space Crisis Exercise (2016)	CSIS/SWF	Inadvertent escalation by accident, inadvertent escalation by miscalculation, advertent escalation	Invest in attribution, increase resilience, reexamine reversibility, set thresholds, demonstrate capabilities
Schriever Wargames, Space Flag, Global Lightning/Thunder	DoD	Classified	Classified

The key takeaway from these previous approaches is that space security concepts can be tested effectively in an unclassified setting, and wargaming in particular can provide valuable insights that are otherwise unobservable in the real world. While these

previous efforts have been useful in expanding our understanding of space security in some way, none of them investigate entanglement as a variable. Tens of millions of dollars have already been spent on disentanglement, but we have never observed the effects of entanglement or disentanglement in an experimental setting. My wargaming scenarios incorporate techniques from the wargaming literature as well as features from previous wargaming scenarios to test the effects of entanglement (IV) on deterrence (DV) for NC3 space systems.

According to Perla, wargames must have the following components: objectives, scenarios, data base, models, rules, players, and ananlysis; all of which are included in my space security wargames.[256] To test my hypotheses, I developed two fictional but realistic geopolitical scenarios and asked participants to assume the role of a senior decision maker from one of three fictional states, Green, Purple, and Yellow. Each of the teams was provided background information which included one of three treatments of the independent variable, entanglement. Teams either had entangled NC3 space systems, disentangled systems, or unknown entanglement status. The latter group served a control to generate a baseline for willingness to attack space systems in general. Prior to scenario execution, teams of two were formed with equal distribution of participants based on major, level of study (PhD/Masters/Undergrad), age, and gender.[257] Several days before the scenario, each team received tailored materials for review and preparation. All teams received a common space security background document that discussed the space environment, the terrestrial environment, space weapons development and testing for

[256] Perla, P. (1990), 30, 180.
[257] Each participant provided consent, and all personally identifiable information was stripped from demographic information in accordance with institute privacy guidelines.

each state, a fictional map of the wargaming world, state military capabilities, options their team could employ, and rules of the scenario. Additionally, each team received a specific background briefing based on the variable they were being evaluated against.

The basic design, state capabilities, background information, and fictional map used in my scenarios were adapted from the CSIS and SWF wargames.[258] I made modifications as needed to address my own research objectives and I developed my own geopolitical scenarios as well as other supporting documents independently to account for my previously untested variables. I also adapted the RAND Corporation's escalation risk matrix to provide greater fidelity with my dependent variable than could be accomplished with a dichotomous treatment of the variable. In addition to a simple count of attacks, I use the risk matrix to assign a severity score for attacks, as the choice by an opponent to use a less severe method of attack could still indicate deterrence was effective in preventing a more severe attack. In addition to the quantitative data gathered during the course of the wargames, I also solicited qualitative feedback from participants following the scenarios regarding the logic underlying their choices

Fictional scenarios and fictional states were required due to the potential security classification issues of using real states and real systems.[259] Additionally, I selected the colors Purple, Green, and Yellow to represent the fictional states since they are not typically associated with good vs. bad or axis vs. allies as other colors might be, like red and blue. CSIS used Blue, Orange, and Yellow as fictional states, but since blue is often

[258] I would like to thank Kaitlyn Johnson from CSIS and Brian Weeden for discussing their scenarios with me, as well as sharing source documents and giving permission to build upon these materials.
[259] As a military member with a security clearance, all of my research has to be reviewed and approved by the Air Force Institute of Technology. The space domain suffers from overclassification and I was strongly cautioned against using real states or real space systems in my research.

used to represent allies, or the "good guys" in wargaming, video games, or other arenas, I chose not to use that color. The goal was to limit each participant's national or cultural biases to the maximum extent possible so that each group believed in the worthiness of their own cause. It would be beneficial to conduct these wargames in the future using real systems and real countries to determine if there are differences in responses, but I had to avoid any possible classification issues. However, I still found that participants embraced their roles and objectives and genuinely wanted to make the best possible decisions for their fictional states.

From August 2020 through April 2022, I conducted a total of 11 wargames, with 3 of these used as research design tests, while the final 8 were used for data collection. The final 8 wargames featured 84 teams and 159 participants from Space Security and Modeling and Simulation classes at Georgia Tech, as well as Air Force ROTC cadets from Georgia Tech and other Atlanta-area schools. A Georgia Tech Institutional Review Board (IRB) approved the scenarios as exempt human subjects research and participants provided oral consent prior to taking part in the scenarios.[260]

Wargames are not without risks and limitations, and Perla highlights some of the common pitfalls encountered in wargames. Perla states that "there is always a possibility that intentional or unintentional advocacy of particular ideas or progams may falsely color the events and decisions made in a game and lead to self-fulfilling prophecies. The designer of a game has great power to inform or to manipulate."[261] This is a risk in many forms of research, but is extremely important to consider to ensure the validity of the wargame. Wargame conductors must take great care to simulate realistic events and

[260] Georgia Tech Institutional Review Board Protocol H20312, Approved 20 August 2020.
[261] Perla, P. and McGrady, E. (2011), 194.

provide inputs that do not force a particular decision or course of action, especially those that might confirm hypotheses. Perla claims that "a wargame's validity can be defined as the extent to which its processes and results represent real problems and issues as opposed to artificial ones generated only by the gaming environment."[262] The actual events in a space conflict scenario might not have occurred in the past, but the geopolitical situations and capabilies of states that are featured in my wargames are certainly based on reality.

3.1.2 Elite Space Security Surveys

In an effort to improve the external validity and generalizability of my research, I also conducted survey experiments using space security elites. While the wargaming scenarios are useful to observe interactions between participants and observe decision making in groups, the population being tested is not the population that would ultimately be called upon to make these decisions. Military members in the space community are also not likely to make the strategic decisions I am investigating, but military leaders are responsible for providing options and recommending actions to the civilians who would make these decisions, so they are a more relevant sample than students. Surveys are a common and useful tool in International Relations because they can be used to assess scenarios and treatments that are impossible or difficult to observe in the real world, while also providing greater access to elite populations than wargaming. Surveys can be conducted globally, asynchronously, and with minimal financial outlays. Surveys also afford researchers precise control over what treatments participants are exposed to and allow for greater randomization amongst participants. Survey data can be captured

[262] Perla, P. and McGrady, E. (2011), 271.

completely virtually and in a standardized format so researchers do not have to fear missing observations and can more easily aggregate data for analysis.

Despite recent research that calls into question gaps between elites and masses in decision making experiments, it is nevertheless accepted within the IR field that elite samples provide researchers with greater validity because elites are the relevant actors to the theory, if the theory involves high-level decision making.[263] Elites can be categorized in a number of different ways, but the classification of military officers as elites, particularly with respect to national security decision making, has been established as a useful approach.[264] I chose to use elites for my survey experiments for two reasons: first, they have occupational relevance, that is, their professions align with the theory being tested. Second, they have cognitive relevance, meaning their expertise is within the domain of the theory being tested.[265] According to Kertzer and Renshon, elite samples are "the most useful when they test theories that directly implicate elites' domain-specific expertise and experience."[266]

One of the most significant challenges with elite samples is access. Because of their prominent positions, elites are generally less available to participate in time-consuming activities like wargaming. They also often have constraints on the types of research they can participate in due to security clearances and other institutional or bureaucratic restrictions. Surveys afford me the opportunity to target a highly relevant population to test my theory while overcoming issues with availability and institutional restrictions. The use of elites for the main survey experiment and non-elites for the

[263] Kertzer, J. (2020); Kertzer, J., and Renshon, J. (2022)
[264] Lin-Greenberg, E. (2021), Jost, T., Meshkin, K., Schub R. (2017); Kertzer, J., and Renshon, J. (2022), 8.
[265] Kertzer, J., and Renshon, J. (2022), 9.
[266] Kertzer, J., and Renshon, J. (2022), 3.

wargaming scenarios and public sample survey also provides me a more heterogeneous sample, which can improve the validity of my research.[267] Some survey experiments have shown substantial differences between elites and non-elites, while others show very little difference, and others fall somewhere in between.[268] Observing differences or similarities between samples can improve the validity of the research and increase its generalizability, or identify potential gaps in the theory being tested.

To develop the elite surveys, I used the background information, geopolitical scenario, and fictional map from my space security wargames and reworked the flow of the information to allow participants to respond with multiple choice and free text answers. As with the wargaming scenarios, there were three treatments of the entanglement IV, and Qualtrics randomly assigned participants to each treatment in an equal distribution. My DV from the wargames, deterrence, is also the DV for the elite surveys and participants had the option to select a variety of space weapons and other non-military actions in response to the scenario they were presented. Survey participants were recruited from private social media pages for members of the U.S. Space Force, U.S. Space Command, and U.S. Air Force Officer Corps, and specifically aimed at people with prior experience operating or working with NC3 space systems. Prior to fielding the primary elite survey, a smaller sample was performed with U.S. Space Force space operations officers to test the research design. In order to comply with Institutional Review Board (IRB) requirements, military members that participated did so as private

[267] Kertzer, J., and Renshon, J. (2022), 17.
[268] Mintz, A. Redd, S., and Vedlitz, A. (2006); Sheffer et al. (2018); Renshon, J. (2015); Kertzer, J. (2020)

citizens in their own free time and not on behalf of or under the direction of the Department of Defense.[269]

3.1.3 Public Sample Survey

In addition to elite surveys, public samples are widely used in the social sciences to gauge perceptions and to understand how public preferences influence government actions. According to Tomz, Weeks, and Milo, "scholars can gain insight into foreign policy by studying the opinions of ordinary citizens."[270] In democratic societies, public opinion can have a significant influence on the actions of political leaders for a number of reasons. Some scholars argue that policies are affected by who the public elects to office and that elected officials attempt to retain their office by making decisions that conform to public will.[271] Others have demonstrated that public officials will align their positions, even on national security issues, to conform to the prevailing public opinion.[272]

Aside from elected officials, military officers have also been shown to consider public opinion when making recommendations about the use of force. Conventional wisdom in the international relations field held that military officers are biased by the nature of the organizations they serve and are likely to recommend offensive doctrines to civilian leaders, which ultimately lead to conflict.[273] While it may be true that military leaders might favor more hawkish policies, they are not immune to the influence of public opinion, and public opinion can have a significant impact on the recommendations these officials make. Lin-Greenberg offers four distinct reasons military officers might

[269] The elite surveys are covered under IRB Protocol H22077 as exempt human subject research, approved 14 March 2022.
[270] Tomz, M., Weeks, J. L., and Yarhi-Milo, K. (2020), 138.
[271] Aldrich, J., et al. (2006); Holsti, O. (2004); Tomz, Weeks, and Yarhi-Milo (2020), 119.
[272] Chu, J., and Recchia, S. (2022), 3-4.
[273] Fearon, J. (1998), 302.

consider public opinion, but ultimately "public support is often seen as a necessary condition for achieving military success."[274] During Vietnam and Somalia, and now most recently in Iraq and Afghanistan, waning public support created significant challenges for military forces, their leaders, and political officials responsible for their employment.[275] Military forces in democratic societies rely on public support for continued funding and recruitment efforts, so it makes sense that military leaders would not want to recommend or take actions that are counter to public opinion.

Applied to my research, these claims suggest that in democratic societies state responses to attacks on satellites, or even the willingness to attack satellites, could be influenced by the public and a public survey can help shed light on these perceptions. In order to assess public perceptions about space system attacks, I fielded a survey that presented respondents with information about attacks on U.S. satellites. Like the wargames and elite surveys, the public survey features the same three treatments of the entanglement IV, yet in the public survey, the language used to describe the entangled systems is less technical. Respondents are then asked to choose from a range of response options, from doing nothing through nuclear retaliation, with a number of other increasingly severe options in between. Respondents are also asked to provide a short answer justification for their selection.

Public survey respondents were recruited through Amazon's Mechanical Turk (MTurk) platform and like the elite surveys, these surveys were hosted on Qualtrics. Qualtrics randomly assigned respondents with an equal distribution across each of the three IV treatments. Non-personally identifiable demographic information such as age,

[274] Lin-Greenberg, E. (2021), 8.
[275] Lin Greenberg, E. (2021), 4.

gender, race, educational attainment, political views, and income were collected from each respondent to allow for additional analysis. The use of MTurk to recruit participants for experimental research has gained momentum in political science and other disciplines in recent years and offers researchers broader and more diverse samples than standard convenience samples, while keeping costs manageable. Additionally, empirical research for online labor markets demonstrates that "MTurk subjects are often more representative of the general population" than standard convenience samples and that "MTurk subjects appear to respond to experimental stimuli in a manner consistent with prior research."[276] The latter point refers to research that compared MTurk worker responses to existing experiments and found that the different populations behaved consistently. The same researchers that performed the comparative analysis also found that MTurk respondents tend to be "substantially more liberal in their ideology" than national averages and are also more knowledgeable of politics.[277] While this could bias a public opinion survey, especially one that involves retaliation, I found no significant differences between respondents based on political ideology, though my respondents did tend to be more liberal on average. The public survey was approved as exempt human subject research by the Georgia Tech IRB.[278]

3.2 Criticisms of Political Science Experiments

As mentioned previously, there have been hundreds of experimental studies published in prestigious political science journals in the last two decades, but in spite of that, there is still skepticism about the use of experiments and "psychological approaches

[276] Berinsky, A., Huber, G., and Lenz, G. (2012), 366.
[277] Berinsky, A., Huber, G., and Lenz, G. (2012), 359.
[278] The elite surveys are covered under IRB Protocol H22125 as exempt human subject research, approved 23 March 2022.

to the study of politics."[279] In particular, the use of students for experimental research in the fields of psychology and political science has been criticized for lacking external validity and generalizability. Nevertheless, it is a common research practice due to availability, proximity, and resource constraints.[280] According to Mintz, et al., "relying on experiments with students "playing" the role of real-world national security policy makers may bias the results," however, Mintz et al. also found that students succeeded in choosing maximizing strategies, while military officers engaged in satisficing, so using students is not fruitless.[281] Students were my best option for wargame participants due to time constraints and availability, but there are also legitimate reasons to prefer students. Most students have not yet been exposed to cultural biases that elites could be constrained by, and they are routinely asked to think critically and innovatively in the academic environment. Additionally, new research calls into question how superior elite samples actually are.

In a recent article, Kertzer uses a meta-analysis of 162 treatment effects between elites and masses and finds that "even if elites and masses differ in their traits and preferences, they generally respond to treatments in strikingly similar ways."[282] He also points to the inconsistent record of elite differences with existing experimental studies, with some showing significant differences in decision making (Mintz, Redd, Vedlitz 2006) some showing significant similarities (Sheffer et al. 2018) and some in the middle (Renshon 2015). As a result, Kertzer concludes that "political scientists have been both overstating the magnitude and misinterpreting the determinants of elite-public gaps in

[279] Kertzer, J. (2020), 1.
[280] Aguinis, H., and Bradley, K. (2014), 352; Kertzer, J. (2020)
[281] Mintz, A. Redd, S., and Vedlitz, A. (2006), 757.
[282] Kertzer, J. (2020), 2.

political behavior" and that "political scientists' reflexive skepticism about experiments conducted on non-elite samples...may be unwarranted."[283] All research requires trade-offs, and this is certainly true when conducting experiments with students, but if differences in responses between elites and masses are not so great as once believed, we can conclude that validity of the research has more to do with design and analysis than the population selected.

That said, in an effort to achieve some level of domain-specific knowledge and cognitive relevance in my non-elite wargaming populations, I recruited students enrolled in international affairs courses, and space policy and security courses. These students do not necessarily have experience making strategic decisions about military operations and the use of force, but they are at least aware of key concepts and should present a more representative, or "ecologically valid" sample than the general public.[284] I also provided all participants in the wargaming scenarios with background and space security overview information to review prior to scenario execution. An elite sample could have increased the validity of my wargames, however, elites are also subject to challenges based on "a host of basic demographic characteristics that have little to do with domain-specific experience."[285]

The use of Air Force ROTC cadets was also a deliberate choice to increase validity and assess differences in decision making amongst similar populations that might be subject to different motivations and cultural influences. Though I do not classify these

[283] Kertzer, J. (2020), 1-3, 22.
[284] According to Lin-Greenberg, Pauly, and Schneider, ecological validity refers to "the extent to which behavior under test conditions mirrors real-world behavior." Lin-Greenberg, E., Pauly, R. and Schneider, J. (2022), 8.
[285] Kertzer, J. (2020), 22.

cadets as space security or military elites, they do serve as a semi-proxy for military officers. Based on previous research, ROTC cadets should exhibit decision making that is at least somewhat consistent with military officers. In Semmel and Minix's 1978 study on small group decision-making for foreign policy, ROTC cadets were utilized in addition to traditional students as well as military officers. ROTC cadets fell in the middle of both groups, as might be expected since they are influenced by both environments.[286] Other studies have used ROTC cadets, retired military officers, or military officers in educational settings as well, which is sometimes a necessary approach when direct access to active-duty service members is not possible.[287]

Ultimately, there are other good reasons to use students for experimental research, beyond cost and availability. One of the interesting revelations from the wargaming done by Herman, Frost, and Kurz that is particularly relevant to my research is the benefit of having participants that are not insiders or elites within the subject being investigated. Outsiders can be useful for analysis because they do not bring the same cultural biases and ingrained doctrine to solving problems. For example, the authors described a post-9/11 global crisis wargame in which U.S. Air Force participants continuously prioritized fighter aircraft and bombers while ignoring what was actually needed in the scenario, which was transport and cargo aircraft to move personnel to support an irregular warfare event.[288] The cultural bias of the Air Force in this case is in no way unique. The importance of culture and doctrine to organizational decision making is well documented in bureaucratic politics literature, especially applied to the DoD and Intelligence

[286] Semmel, A., and Minix, D. (1978)
[287] Kertzer, J., and Renshon, J. (2022), 18; Jost, T. et al. (2017); Friedman, J. et al. (2017)
[288] Herman, M., Frost, M., and Kurz, R. (2009), 258-259.

Community prior to 9/11.[289] As Miles' Law reminds us, "where you stand depends on where you sit."[290] In order to get new perspectives on challenging issues, it is beneficial to have participants who sit in places other than your own. In my wargaming scenarios, cadets and traditional students brought a diverse set of beliefs and backgrounds that are useful in tackling these issues free from the cultural biases of military leaders, policy makers, or academics who have been in the field for many years.

3.3 Summary

The complexity of the space domain and inability to test space security concepts in a real-world environment makes experimental research an effective strategy. In order to test my hypotheses while also increasing external validity of my findings, I chose two distinct but complementary experimental approaches, wargames with students and cadets from Georgia Tech, as well as surveys with both space security elites and public samples. Wargames are effective tools for simulating time pressures, competition, and observing the human interactions and real-time decision making that would occur in an actual crisis. Despite criticisms about the use of students for experimental research in international relations, recent research demonstrates that gaps between elites and masses are not as great as once assumed, and the use of students allows for fresh perspectives on these challenging issues. However, recognizing the value of elite samples, I also use survey experiments featuring the same IV and DV as the wargames to assess decision making by those with both cognitive and occupational relevance. Surveys might lack the valuable interactions that wargaming provides but allow for greater access to relevant populations and more precise control over treatments. In addition to the elite surveys, I conducted a

[289] Allison, G. and Halperin, M. (1972); Halperin, M. (1972); Kier, E. (1995); Zegart, A. (2005)
[290] Miles, R. (1978), 399.

public sample survey to gauge perceptions about attacks on space systems, again using entanglement as my IV.

Taken together, these experimental approaches provide quantitative and qualitative data with which to answer my research question and evaluate my hypotheses. Additionally, the use of diverse populations, amongst both elites and masses increases the external validity of my research. The following two chapters will go further in defining the research design and implementation for each of these methods, as well as present the empirical findings.

CHAPTER 4. SPACE SECURITY WARGAMES

4.1 Wargaming Design and Implementation

The first experimental research instruments I used to gather data were wargames conducted with undergraduate and graduate students at Georgia Tech. My experimental wargames featured two fictional but realistic geopolitical scenarios in which teams competed against an opposing state to achieve their government's stated objectives. Wargame participants were divided into teams of two and were asked to take on the role of a military analyst working for the government of their fictional state, either the Kingdom of Green, Kingdom of Purple, or Republic of Yellow. Participants received briefing packets prior to the scenarios that provided an overview of the geopolitical situation, map of the world, overview of the space and terrestrial environments, background information, team options, and rules. Within the background information, teams were given objectives and were presented with one of the three entanglement treatments (entangled, disentangled, or unknown). In order to directly observe the effects of entanglement on decision making and reduce complexity, no other variables were employed. Information about entanglement status was included within several paragraphs of other team-specific background information and the word entanglememt did not appear in any materials in order to conceal the IV being tested. Teams were also not able to compare briefing packets, so no participants were aware that their briefing materials (and variable) differed from any of the other participants.

Two different geopolitical scenarios were used to ensure the actions of teams were not unique to a certain crisis situation or set of objectives. Scenario 1 involved two fictional states (Green and Purple) in a dispute over Green's expansion and use of islands

previously considered to be in international waters. Purple condemned these efforts historically and deployed maritime forces in the region as a show of force. The scenario begins with Green leadership recommending a campaign to take control of the islands and asking for recommendations from participants, who play the role of senior strategists in the Ministry of Defence, on whether to attack space systems to conceal their military operations from Purple. Purple begins the scenario having collected intelligence that shows Green massing maritime, air, and ground forces and Purple leadership suspecting Green is about to launch a campaign to take the islands. Green makes the first move in this scenario. Yellow is not represented by any teams in Scenario 1, though teams are given background information on Yellow's position in the world and many teams seek alliances with Yellow through the course of the scenario.[291] Scenario 1 is designed to address the prevailing assumption within academia and government that NC3 space systems could be attacked to enable conventional objectives, like claiming islands.

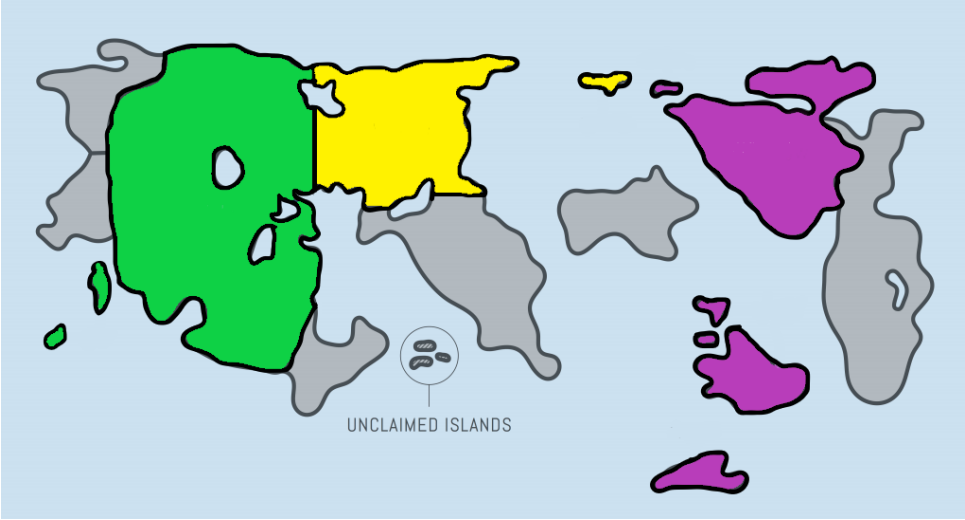


Figure 3 - Scenario 1 Map[292]

[291] Any actions participants take that invoke non-participant states are adjudicated by the white cell.
[292] This fictional map of the world was adapted from the CSIS and SWF wargames conducted in 2016, with permission of the originators.

In the second scenario, Yellow has recently annexed a portion of another state (Orange) on its southern border. Purple has condemned the annexation but not yet taken action out of fear of escalating the conflict with their peer rival. While the crisis unfolds, one of Purple's missile warning satellites in the region malfunctions and attribution for the malfunction does not occur, though Purple leaders suspect a Yellow cyber attack was to blame. The purpose of this initial condition was to observe how teams react to malfunctions with entangled NC3 systems during a crisis, which is one of the concerns that Acton and others point to as a source of inadvertent escalation. Purple moves first so their response to the suspected attack can be clearly observed. As the crisis escalates, teams pursue objectives related either to preserving or reversing the territorial expansion.

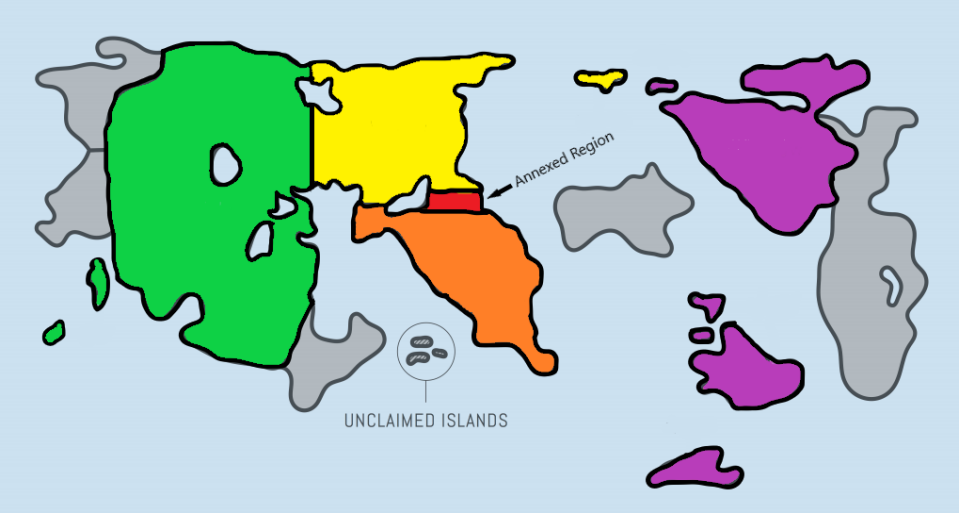


Figure 4 - Scenario 2 Map

As mentioned in Chapter 3, one of the risks of experimental wargaming is researchers leading participants down a particular path, so I intentionally provided participants enough latitude in their options to puruse unique stategies. At the same time, the effects of entanglement on participant decision making needed to be clear in order to assess my hypotheses, so I also took care to ensure treatments of the IV were easy to

understand by participants and sufficiently differentiated amongts groups. Below are samples of the entanglement language included within the team background briefings. With two scenarios featuring two competing states and three entanglement treatments, there are a total of twelve distinct team packets. The full briefing materials for each scenario and treatment are included in Appendix 1, but the statements below (taken from Green team packets in Scenario 1) provide a snapshot into what information teams in each of the entanglement treatments had available. Again, these statements were included within a broader background briefing, so participants were not primed to think this information specifically was being tested.

NC3 Space System Background for All Treatments:[293]

"Purple's intelligence surveillance, and reconnaissance (ISR) and missile warning satellites provide coverage over the islands and would alert Purple leaders to any actions taken by Green to seize the islands. Additionally, Purple's satellite communications (SATCOM) systems allow forward-deployed military forces near the unclaimed islands to communicate securely with Purple leadership globally. Green also possesses ISR, SATCOM, and missile warning satellites to cover the region."

Entangled Treatment:

"The same ISR, missile warning, and SATCOM systems that could be used by Purple to detect and respond to Green's attempts to take control of the unclaimed islands are also part of Purple's nuclear command, control, and communication (NC3) architecture, which provides strategic nuclear warning (i.e. advanced warning of a nuclear attack) and missile defense (i.e. the ability to defend against incoming nuclear

[293] Space Security Scenario 1, Green Versions 1-3

missiles) for Purple. The same applies to Green's ISR, protected SATCOM, and missile warning systems." [294]

Disentangled Treatment:

"Purple and Green have two versions of their ISR, SATCOM, and missile warning systems. One version is part of their nuclear command, control, and communication (NC3) architecture, and is used to support strategic/nuclear missions (like nuclear attack warning and missile defense). The other version of the systems supports tactical/conventional missions, such as Green's campaign to take control of the unclaimed islands and Purple's ability to monitor these actions. Although not their primary mission, NC3 systems may be capable of providing support for tactical/conventional missions, if needed."[295]

Unknown Treatement:

No additional information is provided to participants in this treatment.[296]

During each of three rounds, teams select up to three actions from the list of options provided in their packets. Three rounds and three options per round were necessary due to time and resource constraints, but each participant was also asked to provide additional information after the scenario in order to better understand why they made the choices they did. Ultimately this qualitative data about *why* decisions were made proved to be as useful as observing *what* decisions were made. All teams across all scenarios had the same options available, and these options ranged from diplomatic, informational, or economic actions like sanctions or démarches, to military actions both

[294] Space Security Scenario 1, Green Version 1
[295] Space Security Scenario 1, Green Version 2
[296] Space Security Scenario 1, Green Version 3

in space and terrestrially, kinetic and non. The exception is that teams with disetangled space systems could choose between conventional and nuclear versions of ISR, missile warning, and protected SATCOM systems to attack.

Teams presented their options to the white cell for adjudication and the white cell provided the adjudicated results back to the team and then to the opposing team to allow them to respond. After receiving the opposing team's selections, the white cell again adjudicated the options and provided them to the other team in turn. In this way, teams were responding to the actions of the other team throughout the scenario, which simulates the interaction between states in a crisis. For each of the military actions, teams were provided probabilities of both success and attribution. The probabilities represented realistic assessments of real-world capabilities and were generated by CSIS and SWF for their space crisis wargaming scenarios. These probabilities of success and attribution were necessary to increase the realism of the scenarios but the values were consistent across teams and were not varied during the wargames.[297]

In order to assess the hypotheses, I coded each of the actions taken by participants and used attacks against space systems as a proxy for my DV, deterrence. In addition to a dichotomous treatment of attacks, which is whether or not an attack occurred, I also assigned attacks a severity score to allow for greater context in the quantitative assessment of deterrence. This severity score is based on the escalation risk matrix developed by the RAND Corporation (Table 5, below) for their game-theoretical space control wargaming. By assigning severity scores, I was able to observe possible escalation risks of attacks as well as gain more granularity in assessing my deterrence

[297] The success of attacks and attribution was determined using an excel-based probability simulator.

variable. The choice to use a non-kinetic temporary weapon could still signal deterrence was effective, as the instigator of this type of attack could have been deterred from conducting a more severe attack, even though an attack was conducted. Categorizing attacks and analyzing severity scores provides an additional layer of context on top of simple counts of whether or not attacks occurred, which would be the case if the variable was treated dichotomously.

Table 5 - RAND Corporation Escalation Risk Matrix[298]

My categorization (Table 6, below) shows options available to teams that are counted as an attack against an NC3 space system (or the disentangled version of these systems), as well as categorization by severity.[299] Each of the categories are also given a corresponding multiplier, as in Category 4 has a multiplier of 4, Category 3 has a multiplier of 3, and so on. The most severe category (Category 4) are non-reversible

[298] Morgan, F., et al. (2018), 51. My classification can be found in the research design section of this chapter.
[299] The categorization by severity is based on the RAND matrix on page 76 of this chapter.

kinetic attacks, which include direct-ascent and co-orbital anti-satellite weapons.[300] These weapons are designed to completely destroy target spacecraft and generate significant debris that affects all operators in the orbit, which is why they are most severe and believed to be the most escalatory. The second most-severe category includes non-kinetic, non-reversible weapons (Category 3) which are intended to eliminate system capabilities without creating the same hazardous debris as kinetic weapons. Category 2 attacks include non-kinetic reversible attacks that are intended to inflict outages for a temporary period. Finally, Category 1 includes non-kinetic reversible attacks that are confined to a local geographic area. Instead of the potential far-reaching effects of the related Category 2 attacks, these attacks are intended to disrupt or limit capabilities in a confined area, such as a battlefield.

Table 6, below, identifies and categorizes team options that are counted as attacks against NC3 space systems (and the disentangled versions of these systems). These are the actions that are most relevant for assessing my hypotheses. However, these actions make up only a small percentage of the total options available to teams during the scenarios. Table 7 identifies the totality of actions available to teams, grouped by category, which is how I will present findings in the section that follows. These options were condensed for this section and have greater specificity, like identifying the system to be attacked, in the team briefing packets.

[300] Depending on the source, the term permanent can be used instead of non-reversible, or temporary can be used in place of reversible. I use reversible and non-reversible because that is what the RAND Corporation used in their escalation risk matrix upon which I base my categories.

Table 6 - Attack Severity Classification

Category (Most to Least Severe)	NC3 Space System Attack
4. Kinetic, non-reversible	- Co-orbital ASAT against missile warning/protected SATCOM - Direct ascent ASAT against military ISR - Kinetic attack against missile warning, ISR, or SATCOM C2 or missile warning RADARs
3. Non-kinetic, non-reversible	- Blind missile warning - Blind military ISR
2. Non-kinetic, reversible	- Jam protected SATCOM uplink - Cyber attack missile warning/protected SATCOM/ISR satellites - Cyber attack missile warning, protected SATCOM, or ISR C2 - Cyber attack missile warning RADARs - Dazzle missile warning - Dazzle military ISR
1. Non-kinetic, reversible (localized)	- Jam protected SATCOM downlink

Table 7 - Categorization of Team Options

Category	Action
Diplomatic, Informational, or Economic	- Send public/private démarche - Propose public/private bilateral discussions - Impose economic sanctions - Request military support from allies - Leak information or disinformation to the media
Military Action (Non-space, non-attack)	- Raise/lower the alert status of forces in the region - Deploy/withdraw aircraft in the region - Deploy/withdraw maritime forces in the region - Deploy/withdraw ground forces in the region - Declare a no-fly zone with shootdown authority
Military Attack (Non-space)	- Attack maritime forces - Attack ground forces - Attack air forces - Conduct targeted special operations
Space Action (Non-attack)	- Move co-orbital ASATs near GEO satellites
Space Attack	- Jam SATCOM downlinks (localized) - Jam SATCOM uplinks (wide-area) - Jam PNT signal (localized) - Jam PNT signal (wide-area) - Cyber attack satellites - Cyber attack C2 nodes - Cyber attack missile warning radar(s) - Dazzle/Blind ISR/missile warning satellites - Use co-orbital ASATs against GEO satellites - Use direct-ascent ASAT against LEO ISR and/or MEO PNT satellites - Kinetic attack on C2/SSA/Radar facilities in region/homeland

From Fall 2020 through Spring 2022, I conducted a total of 12 wargaming sessions, 3 of which were used as trial runs to test the overall wargame design and execution and featured a greater number of independent variables. These early sessions were critical for optimizing wargame design and narrowing the variables to ensure results could be linked to what was being tested. The next 9 wargames featured one of the two scenarios mentioned previously, as well as entanglement as the sole IV and deterrence as the DV, as measured through attacks against space systems. The tables below provide an overview of the wargaming sessions, including the number of teams assigned to each treatment, and total number of participants.

Table 8 - Scenario 1 Participants

Wargaming Session	Entangled (# Teams)	Disentangled (# Teams)	Unknown (# Teams)	Participants (#)
Modeling and Simulation Online Class Spring 2021[301]	4	3	3	20
Modeling and Simulation Class Spring 2022	4	4	4	24
Modeling and Simulation Online Class Spring 2022	8	11	0	30
Space Security Class Spring 2022 - Second Round	6	6	0	22
Totals	22	21 (24)	7	96

[301] During this session, I failed to note whether attacks conducted by disentangled teams were against nuclear or conventional versions of systems, so I have excluded these attacks from my analysis in areas where this information is required. In some areas of analysis, differentiation between nuclear and conventional systems is not required, so I include these teams in those sections. Tables in the analysis section will show 34 disentangled teams when these teams are excluded and 37 when they are included. I noticed this error prior to finishing my wargaming sessions and added three teams to the disentangled treatment in a later scenario to even out the totals. Excluding these teams has only a minor impact on overall findings, and if I included the 1 kinetic permanent attack and 4 non-kinetic reversible attacks conducted by these teams, scores for both quantity and severity are raised slightly for the disentangled treatment, which lends more support to my hypotheses.

Table 9 - Scenario 2 Participants

Wargaming Session	Entangled (# Teams)	Disentangled (# Teams)	Unknown (# Teams)	Participants (#)
Space Security Class Fall 2020	2	2	2	12
Air Force ROTC Fall 2020	2	3	3	16
Air Force ROTC Spring 2022	5	5	0	20
Modeling and Simulation Class Spring 2021	2	3	2	15
Space Security Class Spring - First Round 2022[302]	4	4	4	22
Totals	11 (15)	13 (17)	7 (11)	63 (87)

The table below identifies the number of teams in each treatment condition and scenario that I include in my analysis. Again, in cases where it is not important to distinguish between attacks against conventional and nuclear systems, for example when counting total actions taken by teams, I include all 37 disentangled teams. When that information is important, like when assessing attacks against NC3 systems by treatment condition, those teams are omitted. The 12 teams from the Spring 2022 space security class highlighted in grey above are excluded altogether from my analysis due to both the inability to separate participant selections from directed actions, as well as my failure to note which category of systems were attacked by disentangled teams. Additionally, after

[302] During this wargaming session, Yellow teams received additional information that a new administration had been elected and they intended to demonstrate strength and resolve in the space domain and asked participants to conduct an attack against their opponent's NC3 space systems. This input was given to force a response to NC3 system attacks during crisis so I could directly observe which types of attacks were favored as well as the opponent's perceptions about their NC3 systems being attacked. During this session, I also failed to account for whether disentangled teams attacked nuclear or conventional versions of systems. With both of these factors combined, the data from this session were too difficult to classify appropriately and were excluded from my analysis. This is the reason scenario 2 has fewer teams than scenario 1.

the first 6 scenarios, it was very clear that teams with unknown entanglement status behaved consistently, and because this group does not contribute significantly to my hypotheses, I did not include any unknown teams in the final three wargaming sessions. I wanted to maximize the data I gathered for entangled and disentangled teams, so this decision allowed me to do that.

Table 10 - Teams and Participants by Treatment and Scenario

Scenario	Entangled Teams	Disentangled Teams	Unknown Teams	Participants
Scenario 1	22	21 (24)	7	96
Scenario 2	11	13	7	63
Totals	**33**	**34 (37)**	**14**	**159**

4.2 Findings

Prior to delving into the findings from the wargaming, I will briefly review the hypotheses being tested. *H1: Entanglement deters attacks against NC3 space systems.* NC3 space systems are vital assets to the states that possess them, and potential adversaries are aware of the grave consequences they could face for attacking these systems. Attacks against entangled systems, even with conventional aims, affect nuclear capabilities of a targeted state and as such, the risk of massive retaliation and uncontrolled escalation should deter attacks. Under this hypothesis, I expect to see a low number of attacks against entangled systems in general and relative to disentangled systems. *H2: Disentanglement of NC3 space systems makes attacks against conventional versions of the disentangled systems more likely.* Operating on the other end of my argument, disentanglement provides potential adversaries with options to conduct attacks without affecting the nuclear capabilities of the targeted state. As a result, attacks against these systems could be perceived to be less dangerous and therefore become more likely.

I expect to see higher numbers of attacks against disentangled conventional systems relative to entangled systems, as well as fewer attacks against the disentangled nuclear versions of these systems relative to all other groups. With entangled space systems, attackers could still plausibly claim that they did not intend to harm NC3 capabilities, but a disentangled nuclear system removes the veil of ambiguity.

4.2.1 Quantitative Analysis

To set the stage for the analysis of my hypotheses, it is first useful to provide a broad overview of actions taken during the wargaming sessions. Teams were given ample latitude in their options to ensure they were not forced down a particular path, and this freedom of action is evident when examining the data in aggregate. Across wargaming sessions, teams favored diplomatic, informational, or economic actions, which accounted for over 42% of all actions taken. Additionally, teams favored non-attack options over attacks. Out of 669 total actions taken by teams, only 185 (27.65%) involved some type of attack, 37 (5.53%) of which were non-space related attacks, and 148 (22.12%) were attacks against space systems. The graph below provides a snapshot of the total actions taken by teams during the wargaming sessions.

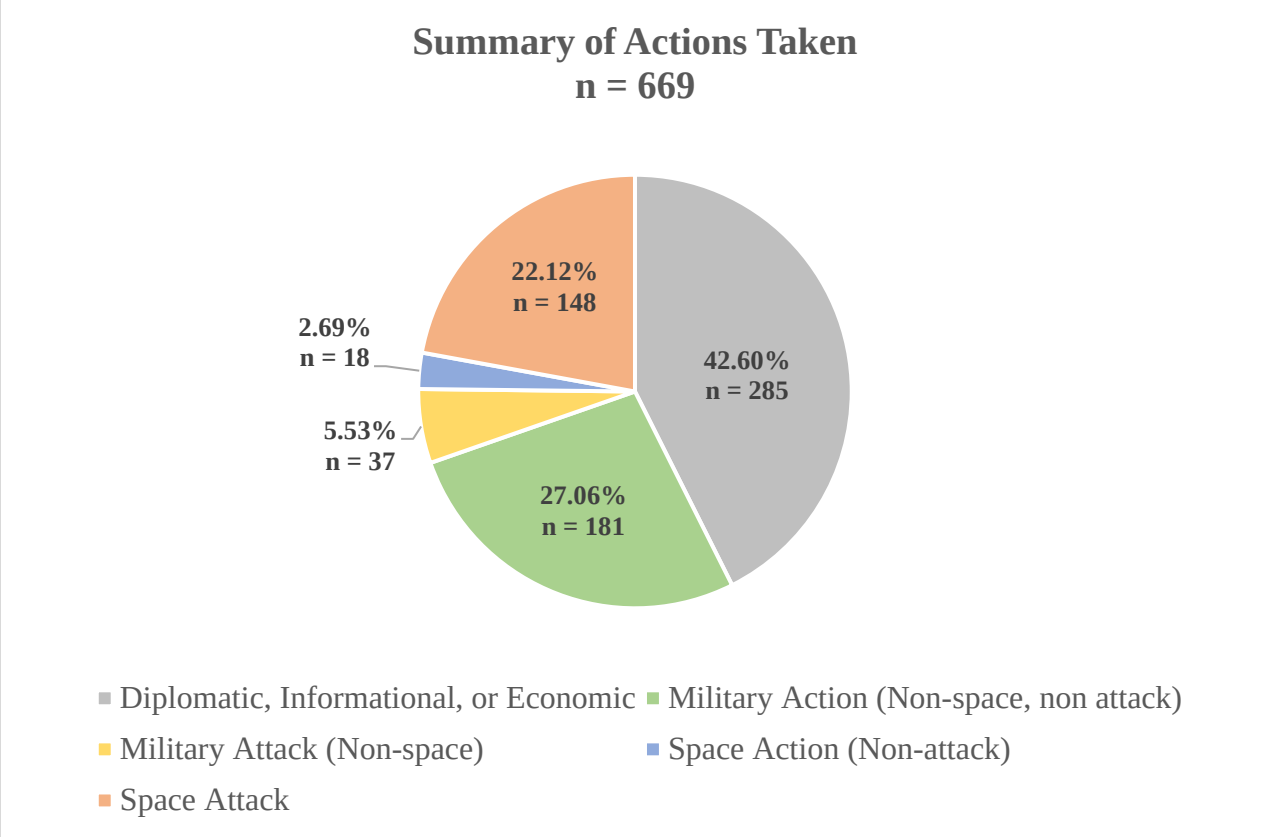


Figure 5 - Summary of Actions Taken

When looking at actions taken by teams in each entanglement treatment, it is clear that diplomatic, informational, and economic actions still take precedence, with the exception being teams in scenario 1 that were unaware of entanglement, who conducted more attacks than anything else. Across scenarios and entanglement treatments, most teams preferred soft power strategies over the use of force. The percentages below the numbers in each of the treatments represent the actions in that category compared to the total actions taken by teams in each treatment.

Table 11 - Actions taken by scenario, category, and treatment[303]

Entanglement Treatment	Diplomatic, Informational, or Economic	Military Action (Non-space, non-attack)	Military Attack (Non-space)	Space Action (Non-attack)	Space Attack
Scenario 1					
Entangled (22 Teams)	88 (49.44%)	64 (35.96%)	5 (2.81%)	1 (0.56%)	20 (11.24%)
Disentangled (24 Teams)	73 (37.63%)	58 (29.90%)	10 (5.15%)	5 (2.58%)	48 (24.74%)
Unknown (7 Teams)	13 (21.31%)	11 (18.03%)	15 (24.59%)	2 (3.28%)	20 (32.79%)
Scenario 1 Totals (n = 433)	174 (40.18%)	133 (30.72%)	30 (6.93%)	8 (1.85%)	88 (20.32%)
Scenario 2					
Entangled (11 Teams)	45 (55.56%)	16 (19.75%)	3 (3.70%)	5 (6.17%)	12 (14.81%)
Disentangled (13 Teams)	46 (48.42%)	19 (20%)	2 (2.11%)	1 (1.05%)	27 (28.42%)
Unknown (7 Teams)	20 (33.33%)	13 (21.67%)	2 (3.33%)	4 (6.67%)	21 (35%)
Scenario 2 Totals (n = 236)	111 (47.03%)	48 (20.34%)	7 (2.97%)	10 (4.24%)	60 (25.42%)
Combined					
Entangled (33 Teams)	133 (51.35%)	80 (30.89%)	8 (3.09%)	6 (2.32%)	32 (12.36%)
Disentangled (37 Teams)	119 (41.18%)	77 (26.64%)	12 (4.15%)	6 (2.08%)	75 (25.95%)
Unknown (14 Teams)	33 (27.27%)	24 (19.83%)	17 (14.05%)	6 (4.96%)	41 (33.88%)
Overall (84 Teams)	**285 (42.60%)**	**181 (27.06%)**	**37 (5.53%)**	**18 (2.69%)**	**148 (22.12%)**

The dispersion of actions across wargaming scenarios is comparable, though numbers are skewed in the military action and military attack categories for scenario 1, possibly as a result of real-world events. One of the scenario 1 wargaming sessions was conducted on 24 February 2022 with students from Dr. Borowitz' Modeling and Simulation class. This was also the day that Russia began their invasion of Ukraine, and

[303] Data for all actions taken by treatment, session, and scenario are provided in Appendix 2.

global news coverage immediately shifted to the crisis. Among the 84 teams who participated in the wargames, there were 37 non-space military attacks conducted. Over half of these attacks (n = 19) were conducted by the 12 teams from that one wargaming session. Fifty-one percent of all non-space military attacks were conducted by just 14% of teams. Additionally, 4 of the 5 non-space military attacks conducted by entangled teams in Scenario 1 were conducted by the 4 entangled teams in that one session, compared to only 1 non-space military attack from the other 18 entangled teams. During this wargaming session, only 1 of 12 teams did not deploy military forces, and fully half of the teams (6 of 12) conducted attacks against ground forces. Conventional attacks against ground forces were selected by only 1 of the other 72 teams (1.39%) that participated in the wargaming scenarios. Despite this dramatic increase in non-space military attacks, attacks against space systems in this session were comparable to other wargaming sessions, so this otherwise outlier data need not be excluded. The table below captures the disparity in military attacks between this session and all others.

Table 12 - Summary of actions taken by category, and wargaming session

Diplomatic, Informational, or Economic	Military Action (Non-space, non-attack)	Military Attack (Non-space)	Space Action (Non-attack)	Space Attack
Modeling and Simulation Online Class Spring 2021 (10 teams)				
25	23	5	3	23
Modeling and Simulation Class Spring 2022 (12 teams)				
31	28	**19**	2	22
Space Security Class Spring 2022 (12 teams)				
48	35	1	0	17
Modeling and Simulation Online Class Spring 2022 (19 teams)				
70	47	5	3	25
Space Security Class Fall 2020 (6 teams)				
27	8	0	3	4
Air Force ROTC Fall 2020 (8 teams)				
19	13	3	2	26
Air Force ROTC Spring 2022 (10 teams)				
40	19	3	3	20
Modeling and Simulation Class Spring 2021 (7 teams)				
25	8	1	2	10
Totals				
285	**181**	**37**	**18**	**148**

A more detailed overall analysis of teams that conducted attacks is also enlightening. Out of 84 teams, 20 (23.8%) did not conduct an attack of any type during the wargames. Interestingly, of the 20 teams that did not conduct attacks, 18 (90%) were from the entanglement treatment and 2 (10%) were from the disentanglement treatment. For comparison, 18 of 33 entangled teams (54.5%) did not conduct an attack of any type during the wargames, compared to 2 of 37 (5.4%) disentangled teams, and 0 of 14 (0%) unknown entanglement status teams. The only two teams not to conduct any type of attack from the Modeling and Simulation session that followed the Russian invasion of Ukraine were entangled teams, and both teams cited fears of nuclear escalation as the primary deterrent for their decisions. Aside from deterring attacks against NC3 space systems, these findings suggest that entanglement could also deter attacks more broadly.

The table below provides greater detail on the attacks conducted by teams within each scenario and entanglement treatment.

Table 13 - Categorization of Attacks by Scenario and Treatment

Entanglement Treatment	Did Not Conduct Attacks	Attacked Space Systems Only	Attacked Non-Space Military Targets Only	Attacked Both Space and Non-Space Targets
Scenario 1				
Entangled (22 Teams)	54.55% (n = 12)	31.82% (n = 7)	0% (n = 0)	13.64% (n = 3)
Disentangled (24 Teams)	0% (n = 0)	70.83% (n = 17)	8.33% (n = 2)	20.83% (n = 5)
Unknown (7 Teams)	0% (n = 0)	14.29% (n = 1)	0% (n = 0)	85.71% (n = 6)
Scenario 2				
Entangled (11 Teams)	54.55% (n = 6)	27.27% (n = 3)	9.09% (n = 1)	9.09% (n = 1)
Disentangled (13 Teams)	15.38% (n = 2)	69.23% (n = 9)	0% (n = 0)	15.38% (n = 2)
Unknown (7 Teams)	0% (n = 0)	57.14% (n = 4)	0% (n = 0)	42.86% (n = 3)

With the high-level overview of team actions in mind, I now look specifically at attacks against space systems in order to address my hypotheses. As a reminder, I code attacks against space systems with both a simple count, as well as a weighted score by severity. For each of these measures I also divide by the number of teams to create a per team average due to the inconsistent numbers of teams within each treatment. A direct comparison without accounting for team differences would not provide an accurate representation. Space system attacks are placed into one of four categories represented by the following symbols: KP (kinetic permanent), NP (non-kinetic permanent), NR (non-kinetic reversible), NL (non-kinetic reversible (localized)), and are divided by T (teams). To calculate the average attacks per team, I simply add the totals from each category and divide by the number of teams. Average attacks per team = (KP + NP + NR + NL) / T

Table 14 - NC3 Space System Attacks by Category and Treatment

Entanglement Treatment	Kinetic Permanent	Non-kinetic Permanent	Non-Kinetic Reversible	Non-Kinetic Reversible (Localized)	Totals (Avg # Per Team)
Entangled (33 Teams)	2	0	12	0	14 (0.42)
Disentangled - Nuclear (34 Teams)	3	0	2	0	5 (0.15)
Disentangled - Conventional (34 Teams)	5	3	32	2	42 (1.24)
Disentangled - Combined (34 Teams)	8	3	34	2	47 (1.38)
Unknown (14 Teams)	8	2	19	0	29 (2.07)
Overall (81 Teams)	**18**	**5**	**65**	**2**	**90 (1.11)**

The table above shows that of all entanglement conditions, disentangled nuclear systems appear to be the safest from attack.[304] This is expected, as an attack against these systems is clearly understood to be the most severe and escalatory. However, it is important to note that in both wargaming scenarios teams did still choose to attack disentangled nuclear systems. Additionally, based on the simple count, entanglement does appear to deter attacks against NC3 space systems relative to other treatments, as only 14 attacks were conducted (0.42 attacks per team) compared to 47 attacks against disentangled systems (1.38 per team) and 29 attacks (2.07 per team) by teams with unknown entanglement status. Disentanglement appears to make attacks against disentangled conventional systems more likely. These findings provide strong support to both hypotheses.

[304] Disentangled systems are separated by category in the table as well as displayed as a consolidated group in the row highlighted in grey.

Absolute deterrence is not achieved with any entanglement condition, but entanglement deterred kinetic attacks more than any other treatment, including when compared to disentangled nuclear systems. Teams that attacked nuclear disentangled systems had already decided to escalate the conflict to full-scale war and intended to cripple their adversary with the highest probability attacks (kinetic) and destroy the most critical systems (nuclear). These findings also provide support to the idea that a motivated adversary will not be deterred from conducting attacks, regardless of entanglement treatments, if they believe the attacks are necessary for their objectives. The table above also shows that non-kinetic reversible attacks were heavily favored across entanglement treatments. Despite lower probabilities of success, teams favored these options because they believed escalation would be less severe and were also concerned about creating harmful debris in space with kinetic attacks. Many teams also cited the lower probabilities of attribution associated with attacks in this category as being a significant motivation for selecting non-kinetic reversible options.

As discussed previously, a simple count of attacks is compelling, but it does not tell the full story of deterrence. A team that conducted a non-kinetic reversible attack could have still been deterred from a more severe type of attack as a result of entanglement. For that reason, I also use a scaled measure of attack severity to assess how entanglement might affect team decision making. This measurement takes a more holistic view of the attacks to try and present an overall score for how severe team actions are, based on entanglement treatment. The numbers in each box below represent the total number of attacks in each category conducted by teams in each treatment. To calculate the severity score, I use the multipliers and categories discussed at the beginning of this

chapter and divide by the number of teams to ensure the most accurate comparison between treatments. The calculation for average severity score per team is:

Severity score per team = ((KP*4) + (NP*3) + (NR*2) + (NL*1)) / T.

Table 15 - Average NC3 Attack Severity Score by Treatment

Entanglement Treatment	Kinetic Permanent	Non-kinetic Permanent	Non-Kinetic Reversible	Non-Kinetic Reversible (Localized)	Severity Score Per Team
Entangled (33 Teams)	2	0	12	0	0.97
Disentangled - Nuclear (34 Teams)	3	0	2	0	0.47
Disentangled - Conventional (34 Teams)	5	3	32	2	2.79
Disentangled - Combined (34 Teams)	8	3	34	2	3.26
Unknown (14 Teams)	8	2	19	0	5.43
Overall (81 Teams)	**18**	**5**	**65**	**2**	**2.70**

The data suggest that disentangled conventional NC3 space systems are not only more likely to be attacked than entangled systems, but they are also more likely to face more severe and escalatory attacks compared to entangled systems. Only two highly destructive kinetic attacks were conducted by the 33 teams in the entangled treatment (6.06% per team average), compared to 8 kinetic attacks from the 34 disentangled teams (23.53% per team average) and 8 by the 14 unknown status teams (57.14% per team average). Of all treatments, teams who were unaware of entanglement status were most likely to conduct kinetic attacks and attacks in general. Interestingly, teams were more likely to attack disentangled nuclear space systems with kinetic weapons than entangled space systems, despite Air Force Space Command's claim that these systems would be

"clearly off limits."[305] Not only does entanglement appear to deter attacks against NC3 space systems from a pure numerical standpoint, but it also appears to deter more severe types of attacks, compared to disentanglement.

Within the category of NC3 system attacks, I also looked at what types of systems were most likely to be attacked, and by what means. The data show that participants overwhelmingly favored attacks against ISR systems, specifically with non-kinetic weapons. Out of 90 total attacks against NC3 space systems, 51 (56.67%) were against ISR, and 42 (82.35%) of these ISR attacks were conducted with non-kinetic weapons. The least popular target among NC3 space systems were protected SATCOM systems, which accounted for only 11 (12.22%) of the 90 attacks. Attacks against missile warning satellites were in the middle with 28 attacks (31.11%). The willingness to attack ISR systems was consistent across entanglement treatments, however there were some important differences with respect to willingness to attack missile warning systems.

Participants generally viewed attacks against ISR as being militarily useful, as well as relatively safe with respect to escalation. This finding was also true for the elite surveys. That was not true for attacks against missile warning, particularly for entangled and disentangled nuclear systems. Of the 33 entangled teams, missile warning systems were only attacked 3 times, and there was only 1 attack against nuclear missile warning systems out of 34 disentangled teams. For 14 teams with unknown status, 10 attacks against missile warning were conducted, and disentangled conventional missile warning systems were attacked 14 times by 34 teams. Missile warning systems appear to be most affected by entanglement due to perceptions that these systems are most likely to lead to

[305] Air Force Space Command (2016), 9.

escalation. This aversion to attacking missile warning satellites, particularly entangled and disentangled nuclear systems, was also evident in the elite surveys, which will be discussed in the next chapter.

Table 16 - Attacks Against Missile Warning Systems by Treatment

Treatment	**Kinetic**	**Non-Kinetic**	**Totals (Avg Per Team)**
Entangled (33 Teams)	1	2	**3 (0.09)**
Disentangled - Nuclear (34 Teams)	1	0	**1 (0.03)**
Disentangled - Conventional (34 Teams)	1	13	**14 (0.41)**
Unknown (14 Teams)	3	7	**10 (0.71)**
Totals (81 Teams)	**6**	**22**	**28 (0.35)**

Table 17 - Attacks Against ISR Systems by Treatment

Treatment	**Kinetic**	**Non-Kinetic**	**Totals (Avg Per Team)**
Entangled (33 Teams)	1	10	**11 (0.33)**
Disentangled - Nuclear (34 Teams)	1	0	**1 (0.03)**
Disentangled - Conventional (34 Teams)	3	20	**23 (0.68)**
Unknown (14 Teams)	4	12	**16 (1.14)**
Totals (81 Teams)	**9**	**42**	**51 (0.63)**

Table 18 - Attacks Against Protected SATCOM Systems by Treatment

Treatment	Kinetic	Non-Kinetic	Totals (Avg Per Team)
Entangled (33 Teams)	0	0	**0 (0.00)**
Disentangled - Nuclear (34 Teams)	1	2	**3 (0.09)**
Disentangled - Conventional (34 Teams)	1	4	**5 (0.15)**
Unknown (14 Teams)	1	2	**3 (0.21)**
Totals (81 Teams)	**3**	**8**	**11 (0.14)**

Table 19 - Comparison of NC3 System Attacks by Treatment

Treatment	Missile Warning (Avg Per Team)	ISR (Avg Per Team)	Protected SATCOM (Avg Per Team)
Entangled (33 Teams)	**3 (0.09)**	**11 (0.33)**	**0 (0.00)**
Disentangled - Nuclear (34 Teams)	**1 (0.03)**	**1 (0.03)**	**3 (0.09)**
Disentangled - Conventional (34 Teams)	**14 (0.41)**	**23 (0.68)**	**5 (0.15)**
Unknown (14 Teams)	**10 (0.71)**	**16 (1.14)**	**3 (0.21)**
Totals (81 Teams)	**28 (0.35)**	**51 (0.63)**	**11 (0.14)**

In addition to assessing attacks against NC3 space systems and the disentangled versions of those systems, I also investigated whether entanglement would affect decisions to attack other types of space systems, like space situational awareness (SSA), position, navigation, and timing (PNT), military satellite communications (MILSATCOM), or commercial systems. The results of this analysis also lend support to my hypotheses, but from a different angle. My theory claims that entanglement deters attacks against entangled NC3 space systems, and when comparing how teams in each of the treatments viewed attacks against other types of space systems, the results show

something interesting. Only teams in the entanglement treatment were more likely to attack these non-NC3 systems, and they did so with a higher severity score than their NC3 system attacks. The other treatments had lower numbers both in total attacks and severity score. While it may seem counterintuitive at first glance, this actually supports my hypotheses. Because entangled teams were deterred from attacking NC3 systems, they felt safer attacking these other space systems, while the opposite is true for the other treatments. Because disentangled teams had safer conventional versions of the NC3 systems to attack, they chose to attack those systems instead of these other space systems. Entangled teams still conducted fewer attacks against other space systems compared to the other treatments, but only the entangled treatment's scores were higher for other system attacks than for NC3 system attacks. This suggests that because entangled teams were deterred from attacking NC3 systems, they chose to attack other systems. Because disentangled and unknown teams were not deterred from attacking NC3 systems, they did not need to target other space systems.

Table 20 - Average attacks on other space systems by treatment

Entanglement Treatment	Kinetic Permanent	Non-kinetic Permanent	Non-Kinetic Reversible	Non-Kinetic Reversible (Localized)	Totals (Avg # Per Team)
Entangled (33 Teams)	3	0	9	6	18 (0.55)
Disentangled (37 Teams)	1	0	16	6	23 (0.62)
Unknown (14 Teams)	2	0	10	0	12 (0.86)
Overall (84 Teams)	**6**	**0**	**35**	**12**	**53 (0.63)**

Table 21 - Severity of attacks against other space systems by treatment

Entanglement Treatment	Kinetic Permanent	Non-kinetic Permanent	Non-Kinetic Reversible	Non-Kinetic Reversible (Localized)	Severity Score Per Team
Entangled (33 Teams)	3	0	9	6	1.09
Disentangled (37 Teams)	1	0	16	6	1.13
Unknown (14 Teams)	2	0	10	0	2.00
Overall (84 Team)	**6**	**0**	**35**	**12**	**1.26**

Summary of Quantitative Data

The quantitative analysis of wargaming data provide support for both hypotheses. A brief recap of the findings is presented with each hypothesis below.

H1: Entanglement deters attacks against NC3 space systems. Quantitative analysis provides support to this hypothesis in several ways. Teams with entangled space systems were less likely to attack NC3 space systems overall and when they did attack, were more likely to use less severe methods. Additionally, entangled teams were significantly less likely to conduct attacks of any kind during the wargaming sessions, with over half of teams (54.5%) choosing not to conduct any attacks, compared to 5% of disentangled teams and 0% of unaware teams. Finally, only entangled teams had increases in scores when assessing attacks against other non-NC3 space systems, indicating a greater willingness to attack these systems both in quantity and severity, despite still having the lowest scores in these categories compared to other treatments.

H2: Disentanglement of NC3 space systems makes attacks against conventional versions of the disentangled systems more likely. This hypothesis is also supported by the quantitative data. Teams with disentangled systems were over three times more likely to

attack conventional NC3 space systems and had average severity scores over three times higher than entangled teams. Disentangled teams were also more likely to conduct attacks against NC3 space systems than other types of space systems, indicating these teams were not deterred from NC3 system attacks. The table below provides a summary of the quantitative analysis.

Table 22 - Summary of Quantitative Analysis

Entanglement Treatment	Avg NC3 System Attacks	Avg NC3 System Attack Severity Score	Avg Other Space System Attacks	Avg Other Space System Attack Severity	% of Teams Conducting Attacks (General)
Entangled (33 Teams)	0.42 (n = 14)	0.97	0.55 (n = 18)	1.09	45.45%
Disentangled Nuclear (34 Teams)	0.15 (n = 5)	0.47	N/A	N/A	N/A
Disentangled Conventional (34 Teams)	1.24 (n = 42)	2.79	N/A	N/A	N/A
Disentangled Combined (34 Teams)	1.38 (n = 47)	3.26	0.62 (n = 23)	1.13	94.12%
Unknown (14 Teams)	2.07 (n = 29)	5.43	0.86 (n = 12)	2.00	100%
Overall (81 Teams/84 Teams)	1.11 (n = 90)	2.70	0.63 (n = 53)	1.26	76.19%

4.2.2 Qualitative Analysis

In addition to the quantitative data collected, I conducted feedback sessions with teams following the wargames to obtain qualitative data about how teams approached the scenarios and most importantly what contributed to their decision on whether or not to attack space systems. The first four wargames had informal discussions following the sessions, which unfortunately meant that not all participants had their voices heard, but the latter five I asked for feedback from each participant, either in email or face-to-face.

In general, the feedback from participants aligns with the quantitative data, although the justifications provided are diverse and interesting in their own right. In the table below, I summarize responses to the question "What was the primary consideration affecting your decision of whether or not to attack space systems?"

Table 23 - Justifications for attacking or not attacking space systems

Primary Consideration	Entangled (n = 40)	Disentangled (n = 39)	Unknown (n = 14)	Responses (n = 93)
Avoid/manage escalation of conflict (general)	37.5% (n = 15)	33.33% (n = 13)	28.57% (n = 4)	33.33% (n = 31)
Avoid/manage escalation of conflict as a result of entangled/disentangled systems	42.5% (n = 17)	15.38% (n = 6)	0% (n = 0)	24.73% (n = 23)
Military necessity/objectives	10% (n = 4)	30.76% (n = 12)	35.71% (n = 5)	22.58% (n = 21)
Response to adversary actions	5% (n = 2)	7.69% (n = 3)	7.14% (n = 1)	6.45% (n = 6)
Deter adversary from future attacks	0% (n = 0)	2.56% (n = 1)	7.14% (n = 1)	3.22% (n = 3)
Likelihood of success	0% (n = 0)	5.13% (n = 2)	7.14% (n = 1)	3.22% (n = 3)
Avoid loss of human life	2.5% (n = 1)	2.56% (n = 1)	0% (n = 0)	2.15% (n = 2)
Keep space peaceful	0% (n = 0)	2.56% (n = 1)	0% (n = 0)	1.08% (n = 1)
Avoid debris creation in space	0% (n = 0)	0% (n = 0)	7.14% (n = 1)	1.08% (n = 1)

The single biggest factor provided by respondents was that they chose to attack or not attack space systems based on the desire to avoid or manage escalation, in general. These participants did not cite any specific characteristics about the spacecraft, like entanglement, that influenced their actions. Rather, they viewed attacks against space systems and escalation from a broad perspective, agnostic of entanglement. It is important to note that this justification is given both as a reason to attack and not attack space systems. Some participants viewed the ability to manage escalation as being a good

reason to attack space systems, particularly with non-kinetic weapons, while others believed the inability to control escalation and the desire to avoid escalation deterred them from attacking space systems.

Following this justification in prominence is a related but more specific group that made their decisions based on characteristics of the systems they intended to attack or avoid, specifically entanglement. Again, for these respondents, this justification was used both for and against attacks. For some, the entangled nature of the NC3 systems caused fears of uncontrolled escalation and deterred attacks, while others said the ability to attack conventional systems and limit escalation made attacks more appealing. It is logical that escalation would be the primary concern of most participants, as that is a primary concern of decision makers in these positions in the real world as well.

Among entangled participants, the most common factor affecting their decision to attack space systems was fear of escalation as a result of entanglement, accounting for over 42% of justifications. According to one participant in the entangled treatment, "The biggest factor of not attacking space systems was the integration of those space systems into the nuclear warning and response systems. Attacking one of these space systems would risk nuclear escalation."[306] Others shared similar concerns saying that "such an attack would be received as highly aggressive, being on the same level if not worse than a ground attack"[307] and "attacking NC3 space systems will be perceived as extremely aggressive and escalatory and will lead to war."[308] The belief that nuclear retaliation was possible and even likely in response to attacks against NC3 systems was shared amongst

[306] Modeling and Simulation Spring 2022, Participant 9
[307] Modeling and Simulation Spring 2022, Participant 3
[308] Space Security Spring 2022, Participant 8

many participants. I will provide more data on that in the subsequent section, but several participants said things to the effect of "If secure access to NC3 is taken away, that represents an existential threat to a country and nuclear retaliation should be expected."[309]

Participants from disentangled teams were also concerned about escalation, though many viewed conventional systems as having a lower risk of escalation and greater flexibility in managing escalation. One participant said that "nuclear systems have to be avoided, but cyber attacks against conventional systems can probably occur regularly without much problem."[310] This participant believed it likely that these types of attacks were already occurring, but were not visible to the public. Another participant said simply "Of course it is safer to attack a conventional missile warning satellite than a nuclear one."[311] Overall, escalation was the primary factor given by 80% of entangled teams, compared to 48.7% of disentangled participants, and 28.6% of unknown status participants. This would be expected based on my theory that entanglement deters attacks against space systems due to fears of severe retaliation and escalation. Again though, escalation was given as a justification both to attack and abstain from attacking.

Across entanglement treatments, participants provided other diverse reasons to attack or not attack space systems. A couple of participants shared the view that attacks against space systems "can't be that serious because human lives are not lost."[312] Another participant said that "attacking space systems seemed like a safe show of power because it didn't cause any loss of life."[313] Other participants believed that attacks against space

[309] Modeling and Simulation Online Spring 2021, Participant 4
[310] Modeling and Simulation Online Spring 2021, Participant 5
[311] Space Security Fall 2020, Participant 1
[312] Air Force ROTC Spring 2022, Participant 2
[313] Space Security Spring 2022, Participant 2

systems will be the new normal in conflict, with one claiming that "anyone who wants to win 21st century battles will attack space systems."[314] A number of participants said that the decision all boiled down to military objectives, and attacking space systems can be decisive in that regard. This was the primary factor given by participants in the unknown treatment. According to one Air Force ROTC cadet, "space system attacks are attractive, particularly as a militarily inferior state, due to the asymmetric effects that can be achieved."[315] Another participant said that it was an easy decision to attack space systems because "you have a better chance at achieving your military objectives while minimizing casualties."[316]

Many other participants who attacked space systems did so in retaliation for attacks against their own systems. One participant said "we believed the adversary created an environment of hostility so we decided to go on the offensive and attack them in the same manner they did us."[317] Retaliation for attacks was a key factor for many teams when making decisions, though it was only cited as the primary motivation by 6 of 93 respondents. When looking back at team actions though, the data show that teams who had not previously conducted an attack retaliated in-kind (either with the same type of weapon or against the same type of system) 73% of the time; 18% of teams did not retaliate, and 9% retaliated in a different manner than they were attacked. It is not possible to say whether or not these attacks were in direct retaliation, or if the teams would have conducted the attacks in that round anyway, but there was a tendency to

[314] Space Security Spring 2022, Participant 18
[315] Air Force ROTC Spring 2022, Participant 1
[316] Modeling and Simulation Online Spring 2021, Participant 7
[317] Space Security Spring 2022, Participant 5

retaliate in kind when faced with an attack. This proportional response tendency will surface again in the public survey section of the next chapter.

Some variation of the comments above were fairly common across wargaming sessions. There were, however, some other unique justifications provided for attacking or not attacking space systems. One participant said it ultimately came down to them "not wanting to be the first person to start a war in space."[318] A couple of other participants said that the uncertainty of how attacks would be perceived and what retaliation might occur made them question attacks against space systems, though one of these groups did conduct attacks, while the other didn't. For the group that didn't conduct attacks, their reasoning was that the "fear of how attacks would be responded to" outweighed whatever they hoped to achieve.[319] The group that did conduct attacks said that "there's an undefined level of retaliation, so it's extremely dangerous and scary, but in some cases it's a better option than terrestrial attacks."[320]

A few participants brought up a possible deterrent value of attacking space systems, including one Air Force ROTC cadet who stated that they chose to attack space systems first to "deter the opponent from attacking mine."[321] They believed that the best defense was a strong offense, and that demonstrating capability and resolve early would deter attacks against their systems in the future. Ultimately that was not the case, but the justification is both valid and interesting. Out of all respondents, only one participant indicated that debris creation was the primary factor in their decision to attack space systems, and they did so using non-kinetic means.

[318] Modeling and Simulation Online Spring 2022, Participant 25
[319] Space Security Fall 2020, Participant 2
[320] Modeling and Simulation Online Spring 2022, Participant 1
[321] Air Force ROTC Spring 2022, Participant 3

In addition to justifications for attacks, some respondent provided justifications for the types of attacks they conducted. Across all entanglement treatments, some methods of attack, particularly cyber, were perceived as especially safe. One participant addressed cyber attacks from a unique perspective and said that "cyber attacks were less visible so they demanded less of a severe response, as they allowed the other country to conceal the attack from their public and not be forced to escalate."[322] From this person's perspective, cyber attacks could be employed by states to signal threats, resolve, or capability to each other without the public ever being aware this was happening, which would provide more flexibility to decision makers on whether and how to respond. Another participant from the same session agreed and echoed that "cyber *feels* like a less aggressive domain in general."[323] Other participants were attracted to the difficulty in attributing cyber attacks claiming that "cyber attacks give you the opportunity to deny your involvement while testing out your adversary and the battlespace."[324] Another participant made the decision to conduct cyber attacks with their teammate due to their belief of how the attack would be perceived. They stated that "cyber attacks may be psychologically less threatening than other types of attacks and for that reason we thought they provided the right trade-offs for subversion with less escalation and attribution."[325] Whatever the reason, cyber attacks were extremely popular across treatments, accounting for 42.57% of all space system attacks.

[322] Space Security Fall 2020, Participant 5
[323] Space Security Fall 2020, Participant 8
[324] Modeling and Simulation Online Spring 2022, Participant 6
[325] Modeling and Simulation Online Spring 2022, Participants 12 and 13

4.3 Other Findings

One of the concerns about entanglement brought forward is that a satellite malfunction during a crisis could cause states to misperceive that an attack had occurred and escalate inadvertently.[326] With any complex system, there is an assumption that despite best efforts, at some point anomalies and failures will occur. These so-called "normal accidents" cannot be avoided, and increased system complexity and safeguards could actually make them even more likely.[327] To test the likelihood of inadvertent escalation resulting from a system malfunction, I gave Purple teams in Scenario 2 the following input in their background briefings: "While these events are unfolding, a Purple missile warning satellite that provides coverage over the southern border of Yellow has stopped functioning. Purple military leaders believe the system has been attacked with an offensive cyber weapon in order to obscure further military action in the region, but attribution and confirmation of the attack has not occurred."

Based on the claims of inadvertent escalation, I expected Purple teams (regardless of treatment) to retaliate as if the malfunction was the result of an attack. That did not occur, however. Of the 37 Purple teams that received this input, only 4 teams (10.81%) conducted attacks in their opening round moves. Of the 4 attacks, 2 were conducted by disentangled teams, 2 were conducted by unknown status teams, and 0 were conducted by entangled teams. According to participants, there was a tendency to assume that the malfunction was the result of a deliberate attack, and those that counter-attacked did so based on that assumption. Others felt it was too risky to treat the malfunction as an attack without attribution. Ultimately, these findings cast doubt on whether states would

[326] Zhao, T. and Bin, L. (2017), 61; Acton, J. (2018)
[327] Perrow, C. (1999).

retaliate to system malfunctions without attribution, even during crises. The findings also reinforce the critical importance of investing in capabilities, like space domain awareness (SDA), to improve attribution.

Another interesting finding related to the credibility of threats in response to NC3 space system attacks. As mentioned in Chapter 2, the U.S.' 2018 Nuclear Posture Review states that nuclear retaliation is possible in response to attacks against NC3 space systems, but it is unclear whether or not this threat is perceived as credible by potential adversaries. I used similar language to the NPR in the background briefings provided to teams ahead of the wargames and in an effort to better understand the credibility of this threat, I presented the question of credibility to wargaming participants following the sessions. The purpose of asking this question was to better understand not only if the existing policies are credible, but also to better evaluate this aspect of the logic that underlies my theory.

The vast majority of participants believed the threat of nuclear retaliation in response to attacks against NC3 space systems to be credible. While responses varied, many participants made the point that an attack against NC3 space systems does not make sense unless an adversary intended to cripple a state's ability to respond to a nuclear attack. According to one participant, "attacking NC3 can be indicative that a nuclear attack is imminent, and the opponent wants to disable second-strike capability."[328] Another participant believed that "the only reason why an actor would attack your NC3 would be to utterly cripple your national defense" and therefore it "seems credible to threaten massive repercussions in order to defend that critical

[328] Modeling and Simulation Spring 2022, Participant 7.

infrastructure."[329] Yet another student pointed to the conflict between Russia and Ukraine, and the West's hesitancy to intervene as being proof that nuclear retaliation is a very real and credible threat. According to this participant, "people in power are so unpredictable and since they can't be predicted, you have to take them at their word because the risk is too great otherwise."[330] This comment harkens back to the threat that leaves something to chance. Even if unlikely, the mere possibility of nuclear retaliation could be strong enough to deter all but the most committed attacker.

The majority view held that threatening nuclear retaliation was credible, but 19% of participants did not believe this to be the case. The consensus among this group was that nuclear weapons are just so incredibly destructive that it is impossible to imagine them being used in the future, for any reason. These participants believed a threat to use the weapons was inherently un-credible because no state would follow through on the threat. According to one participant, "it is never credible for a state to threaten nuclear retaliation, because I don't believe a state would ever use nuclear weapons."[331] Another participant argued that "there are other more morally sounds means of retaliation" so nuclear retaliation shouldn't even be on the table.[332] Ultimately, there is no absolute consensus on whether nuclear retaliation is a credible threat, but the responses at least tell us that for some portion of the population, the threat should be heeded. This is an important belief to understand as my argument for deterrence through entanglement is predicated on the assumption that adversaries expect a severe and unacceptable level of retaliation and escalation in response to attacks against NC3 space systems. While

[329] Modeling and Simulation Spring 2022, Participant 13.
[330] Modeling and Simulation Online Class 2022, Participant 2.
[331] Space Security Class Spring 2022, Participant 3.
[332] Space Security Class Spring 2022, Participant 4.

nuclear retaliation would be the most severe consequence imaginable, a majority of wargaming participants believed it to be possible. A summary of the responses is provided in the table below.

Table 24 - Credibility of Nuclear Retaliation Threat

Is it credible to threaten nuclear retaliation for attacks against NC3 space systems?	**Responses (n = 79)**
Yes	67.09% (n = 53)
No	18.99% (n = 15)
Only if nuclear capabilities were totally crippled by an attack	6.33% (n = 5)
Unsure	3.80% (n = 3)
Only if attribution and intent can be known	2.53% (n = 2)
Depends on the state making the threat	1.27% (n = 1)

The wargaming scenarios also demonstrated a willingness by a majority of participants to employ space weapons in conflict, and I was curious whether or not participants believed that employing space weapons in a real-world conflict would be considered taboo. This does not address whether or not participants would employ these weapons, rather how they believed the employment of these weapons would be viewed by others. The purpose of asking this question was to gain more insight into perceptions about space system attacks. I wanted to better understand if other factors could be at play that affected participants' decisions to employ space weapons. The responses to this question were very interesting and provided much greater insight into views on space weapons. Some participants believed that attacks against space systems would be taboo because of the sanctuary of space (or at least perception of space sanctuary) that has

persisted for decades. According to several participants, kinetic attacks would be taboo, but non-kinetic attacks would be acceptable. One participant went so far as to claim that "as long as no debris is created then it's fair game."[333] For others it was a matter of what type of system was attacked, more than how. According to one participant, it was safe to conduct attacks as long as you "steer clear of anything that has a nuclear flavor to it."[334]

As was the case in attack justifications, cyber attacks again received special mention. One participant said "attacking space systems is still a relatively new frontier and therefore doesn't carry much of a taboo with it" and "cyber-attacks are so commonplace that a cyber-attack directed at a satellite would not be seen as particularly egregious."[335] Many others shared the belief that cyber attacks were not particularly destructive, and "should be expected."[336] A couple of participants believed that the taboo would be based on who was conducting the attack and who was attacked. According to one of these participants, space system attacks would only be viewed as taboo within Western democracies.[337] Finally, one participant said that like other domains, we should expect military space systems to be viewed as legitimate targets and therefore be attacked in future conflicts. This participant believed that whether or not attacks would be considered to be taboo is irrelevant because "they might be required to limit the military capabilities of another country."[338] The table below summarizes responses to the question of whether or not attacks against space systems would be taboo.

[333] Modeling and Simulation Class Spring 2022, Participant 6.
[334] Modeling and Simulation Online Class Spring 2022, Participant 4.
[335] Space Security Class Spring 2022, Participant 12.
[336] Modeling and Simulation Class Spring 2022, Participant 5.
[337] Modeling and Simulation Online Class Spring 2022, Participant 3.
[338] Space Security Class Spring 2022, Participant 16.

Table 25 - Perspectives on whether space system attacks are taboo

Are attacks against space systems taboo?	Responses (n = 79)
Yes	44.30% (n = 35)
No	26.58% (n = 21)
Depends on the type of attack	15.19% (n = 12)
Depends on public awareness	8.86% (n = 7)
Depends on state conducting the attack	2.53% (n = 2)
No for military systems, yes for commercial/civil	1.27% (n = 1)
Unsure	1.27% (n = 1)

4.4 Constraints and Limitations

In addition to some of the limitations of experimental research discussed in Chapter 3, as well as criticisms on the use of students for experimental research, there are other limitations and constraints with the wargaming scenarios and my analysis of the data. One of the major limitations affecting this research was the need to constrain wargaming sessions to three rounds. A number of participants mentioned the difficulty in achieving complex objectives in such a short period, and future research might benefit from conducting full-day or at least extended sessions. Additionally, some participants wanted to select more than three options during the rounds. I chose to limit the choices to three partially in order to account for the time limitations, but also to have more consistency in the data across teams, sessions, and treatments.

Another limitation in the data is that severity scores do not account for participant perceptions or types of systems attacked. A cyber attack against a missile warning system is likely to be perceived as more severe than a cyber attack against an ISR system, though

for my research these attacks are treated the same. A kinetic attack against a nuclear satellite would most likely be more severe than a kinetic attack against a conventional satellite, though again I place the same severity multiplier on these attacks. Ultimately, it is impossible to predict how different attacks against different types of systems would be perceived, because even in the real world this would be affected by the context of the attack, the impact of the attack, the personalities of the leaders involved, and hundreds of other factors. Conducting these wargames using real systems and real states could potentially alleviate some of this, but still participants would be responding to best guesses of adversary intentions. Both the quantitative and qualitative data partially addresses this concern, as participants clearly avoided some types of attacks against some systems, namely kinetic attacks against entangled/nuclear missile warning systems. Many of these participants also provided feedback to support their perceptions of severity.

4.5 Conclusion

The wargames lend strong support to both hypotheses. Entangled teams were not only a third as likely to attack NC3 space systems as disentangled teams, when they did conduct attacks, they did so with less severe methods. Additionally, feedback from participants suggests that fear of uncontrolled escalation and retaliation was the primary determinant for their decision to attack or not attack NC3 space systems. Not only were entangled teams less likely to attack space systems, they were also less likely to conduct attacks of any kind. While my theory does not purport to extend beyond NC3 space systems, it is possible that entanglement could have a broader deterrence effect when potential adversaries view disabling these systems as a necessary condition to achieve

their objectives. In this case deterring attacks against NC3 space systems also deters the broader objective.

For the second hypothesis, disentangled teams were much more likely to conduct attacks against disentangled conventional systems, and did so with greater severity. Feedback from participants suggested that these disentangled systems provided a safer alternative with more room for managing escalation. That said, disentangled teams did still conduct attacks against nuclear systems, so even if disentanglement was pursued as a strategy, there is no guarantee that nuclear systems would be safe. Participants suggested that in order to be certain that an adversary's capabilities were degraded, they could not rely on disabling only conventional/tactical versions of systems, as the strategic/nuclear versions could still provide the data or services that they were trying to interrupt.

Another important finding that will be emphasized in the next chapter is that not all space systems or types of attack are viewed equally. Participants across treatments were far more likely to attack ISR than missile warning or SATCOM systems and were likely to do so with non-kinetic weapons. There was a general consensus among participants that cyber weapons were the least dangerous of all and should be expected to play a significant role in future conflicts. Despite lower probabilities of success compared to kinetic weapons or other types of non-kinetic weapons, participants favored the increased ability to conduct attacks without attribution compared to other methods. Cyber attacks were also viewed by both attackers and victims as necessitating a less severe response, compared to other types of attacks. Again, this trend will be echoed by the survey experiments in the chapter that follows.

CHAPTER 5. SPACE SECURITY SURVEY EXPERIMENTS

5.1 Elite Survey

5.1.1 Elite Survey Design and Implementation

As discussed in Chapter 3, I developed and fielded two experimental surveys; one to test my hypotheses on an elite sample population, and the other to gauge public perceptions regarding attacks against space systems, and what kinds of responses would be supported. I will begin with the elite survey and conclude this chapter with the public sample survey. The elite survey I fielded utilized the background information, map, and treatment conditions from the wargames, but with constrained attack and response options available to respondents. The survey was conducted with space elites (n=76) using the Qualtrics survey platform, and participants were recruited through private space professional social networking sites. To improve the quality and validity of survey findings, I instituted a treatment check at the end of the survey to gauge whether respondents understood the information that they were being exposed to. Of the 76 participants who fully completed the survey, 58 (76.32%) passed the treatment check. The failures were roughly equal in each treatment condition, so the entangled, disentangled, and unknown treatments had 19, 19, and 20 validated complete responses, respectively.

In both the wargaming scenarios and the survey, respondents are asked to take on the role of a space strategist, so the relevant population I targeted were field-grade officers (FGOs) in the military space community who currently are or would likely serve as strategists for real-world events. I also targeted U.S. Space Force officers in the space operations career field to ensure that a majority of survey participants had experience

working with NC3 space systems directly. Qualtrics randomly assigned respondents to each of the three treatment conditions and the demographic data I collected from participants show a roughly equal distribution of participants across treatments based on service, rank, NC3 experience, and gender. The exception is that respondents with no NC3 experience were overrepresented in the unknown treatment. Across all treatments, FGOs accounted for 87.93% (n =51) of respondents, and a majority of respondents (62.07%) had experience working with NC3 systems. United States Space Force (USSF) members comprised 53.45% (n =31) of respondents with United States Air Force (USAF) members next with 39.66% (n =23). The United States Army (USA) and Royal Australian Air Force (RAAF) each had one participant. The table below provides an overview of the demographic information of respondents and composition of treatment groups.

Table 26 - Demographic information for elite survey respondents

Treatment	Service	Rank	NC3 Experience	Gender
Entangled (n = 19)	USSF: 10	FGO: 17	Yes: 14	Male: 16
	USAF: 8	CGO: 1	No: 4	Female: 2
	Unk: 1	NCO: 1	Unk: 1	Unk: 1
Disentangled (n = 19)	USSF: 10	FGO: 17	Yes: 12	Male: 16
	USAF: 7			
	USA: 1	CGO: 2	No: 7	Female: 3
	RAAF: 1			
Unknown (n = 20)	USSF: 11	FGO: 17	Yes: 10	Male: 15
	USAF: 8	CGO: 2	No: 9	Female: 4
	Unk: 1	Unk: 1	Unk: 1	Unk: 1

To begin the survey, respondents in all treatments are presented with the same background information. The scenario was designed to portray a regional conflict between two peer rivals and feature some potential military advantage for attacking space

systems. This is the type of scenario many in academia and within government fear as being a likely, or at least plausible, avenue for NC3 space systems coming under attack in future conflicts. In order to assess the impact of various entanglement treatments, I needed respondents to be forced to make a choice about attacking space systems, so the background briefings led respondents up to the point of making that decision. Like the wargaming scenarios, this survey utilized fictional states and notional capabilities to avoid issues with classification, though as will be discussed later in the chapter, some respondents applied their existing knowledge of real-world systems, capabilities, policies, and strategy to the survey. Below is the briefing that all respondents received.

All Treatments:

"You are a senior space strategist in the Ministry of Defense in the Kingdom of Green. Your country's leaders want to use military force to seize control of disputed islands located in international waters (pictured above). Your peer competitor, Purple, has threatened military intervention if Green attempts to take control of the islands.

Purple's intelligence surveillance, and reconnaissance (ISR) and missile warning satellites provide coverage over the islands and would alert Purple leaders to any of your country's military actions. Additionally, Purple's satellite communications (SATCOM) systems allow forward-deployed military forces to communicate securely with Purple leadership globally.

Some members of your country's leadership believe that attacking Purple's ISR, missile warning, and SATCOM satellites could allow your forces to seize control of the islands without early detection by Purple.

Your country's objectives are limited to gaining control of the islands and do not seek a broader confrontation with Purple."

Following the information above, respondents were provided with additional details based on the treatment they were assigned to. However, I designed the Qualtrics survey to show the briefing above as well as the specific information below as one

continuous background briefing to ensure respondents weren't clued into the variable being tested. The treatment-specific statements are provided below.

Entangled Treatment:

"Purple's ISR, missile warning, and SATCOM systems that could be used to detect/observe Green's campaign and support Purple operations are also part of Purple's nuclear command, control, and communication (NC3) architecture, which provides strategic nuclear warning and missile defense for Purple.

Purple's stated policy is that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation for attacks against NC3 systems.

The Kingdom of Green has the ability to attack space assets using the methods shown in the table below. Your leadership has asked for your recommendation on how to proceed."

Disentangled Treatment:

"Purple has two sets of ISR, SATCOM, and missile warning satellite systems. One set of satellites supports tactical/conventional missions, like operations to detect and stop Green from taking control of the disputed islands. The other set of satellites is part of their nuclear command, control, and communication (NC3) architecture, which provides strategic nuclear warning and missile defense for Purple. Although it is not its primary mission, the NC3 systems may be capable of providing support for tactical/conventional missions, if needed.

Purple's stated policy is that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation for attacks against NC3 systems.

The Kingdom of Green has the ability to attack space assets using the methods shown in the table below. Your leadership has asked for your recommendation for how to proceed."

Unknown Treatment:

"Purple's stated policy is that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation.

The Kingdom of Green has the ability to attack space assets using the methods shown in the table below. Your leadership has asked for your recommendation for how to proceed."

As with the wargames, respondents were provided with the fictional map of the scenario:

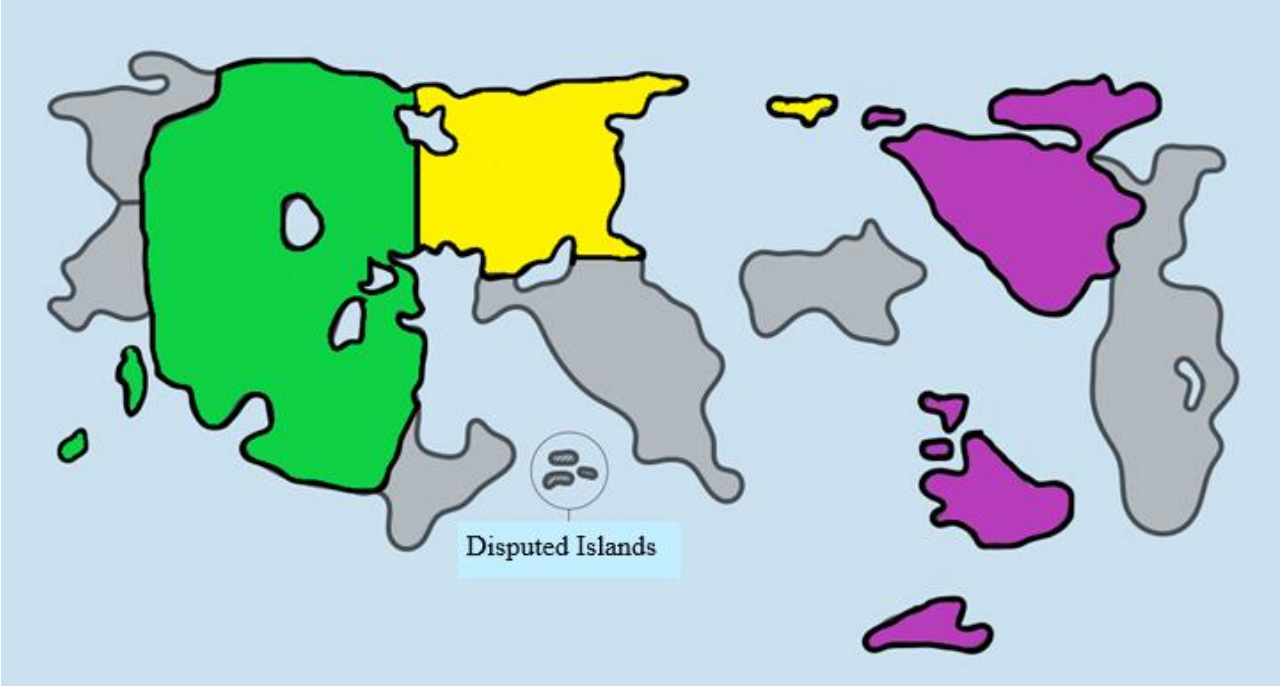


Figure 6 – Elite Survey Map

Finally, each respondent was provided a summary table of the various space attack options available to them. Despite working in the military space community, respondents have varied backgrounds and varying levels of familiarity with space weapons, so this table was necessary to ensure a common level of understanding. Additionally, I again utilized the percentages of success and attribution developed by CSIS and SWF with each of the space attack options to provide greater realism.

Table 27 - Attack descriptions for survey respondents

Type of Attack	Description	Likelihood of Success	Probability of Attribution (Likelihood Purple will know Green carried out the attack)
Kinetic Permanent	An anti-satellite weapon (missile or object in orbit) collides with the adversary satellite and destroys it.	90%	90%
Non-Kinetic Permanent	A laser is used to permanently disable ("blind") an ISR or missile warning sensor.	70%	80%
Non-Kinetic Temporary	A laser is used to temporarily disable ("dazzle") an ISR or missile warning sensor *OR* a communication device is used to temporarily disable (jam) the ability to communicate with a satellite.	90%	80%
Permanent Cyber Attack	A cyberattack is used to permanently disable a satellite on orbit or permanently disable the ability of ground systems to control and communicate with the satellite.	60%	50%
Temporary Cyber Attack	A cyberattack is used to temporarily disable a satellite on orbit or temporarily disable the ability of ground systems to control and communicate with the satellite.	70%	50%

After reviewing background information, all respondents were asked the question: "Do you recommend attacking Purple's missile warning, ISR, and/or SATCOM systems?" It was important to ask this question directly to enable a clearer test of my hypotheses. If respondents selected "no," they bypassed the next three questions and were asked to write a sentence or two explaining their reasoning. If respondents selected "yes," they were then asked "Which system(s) would you choose to attack (select all that apply)?" The response options for this question were the same for entangled and unknown treatments, but disentangled treatment respondents were able to select between strategic/nuclear and tactical/conventional versions of disentangled NC3 space systems. Respondents were then asked to select what type of attack they were most likely to employ, identified in Table 27, above.

This initial set of questions is what I used to determine the effect of entanglement on deterrence and assess my hypotheses. However, I also wanted to better understand and evaluate the theory that underpins my hypotheses, so I asked respondents to answer a series of questions that gauge perceptions about space system attacks and policies about retaliation. Following the questions above, respondents were asked to assess the most likely response if Purple's NC3 space systems were attacked, as well as Green's most likely response if their NC3 space systems were attacked. Again, the disentangled treatment received two versions of these questions, one with nuclear/strategic systems being attacked, the other set with tactical/conventional systems being attacked. Respondents chose from one of nine available options with increasing severity. The options for these questions are provided below (only the country changes based on who was attacked):

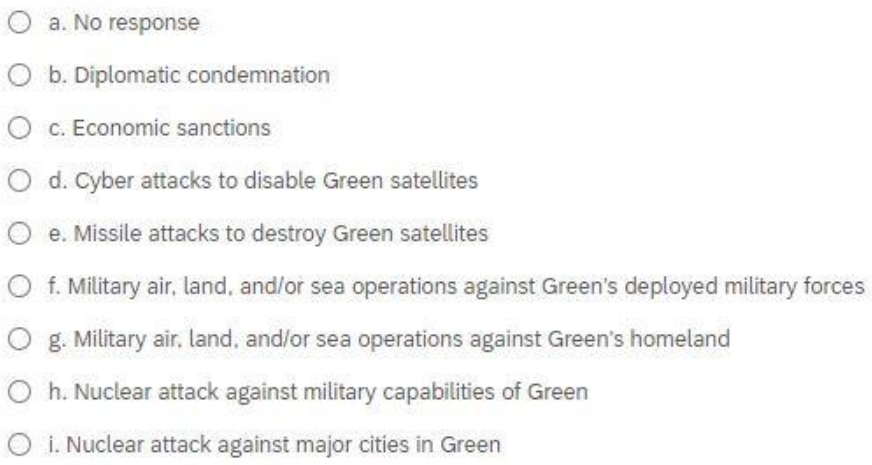


Figure 7 - Survey response options for attacks

The benefit of using this consistent set of responses that have varying levels of severity is that participants were only able to select the most likely response, and I was able to assign numerical values to each of these responses, from 1-9, to enable a simpler quantitative analysis of otherwise categorical data. Additionally, I used the same response options for the public surveys which will be discussed next, so the data are complementary.

Finally, to test the aspect of my theory that addresses credibility of threats, as well as to better understand how respondents view the existing policy of the U.S. that attacks against NC3 space systems could be met with nuclear retaliation, I asked: "How credible do you believe it is that Purple would respond to attacks on their NC3 space systems with a nuclear attack (assume the attack crippled NC3 capabilities)?" I asked this from the perspective of the attacking state assessing victim state threats, because I wanted to better understand whether this type of threat is believed, and whether those beliefs might affect the deterrence value of the threat. Because respondents in the unknown treatment condition were not told any information about NC3 systems, they were asked a more

general version of the question: "How credible do you believe it is that a state would respond to attacks on their Nuclear, Command, Control, and Communication (NC3) space systems with a nuclear attack (assume the attack crippled NC3 capabilities)?" Respondents were asked to select from one of the following options:

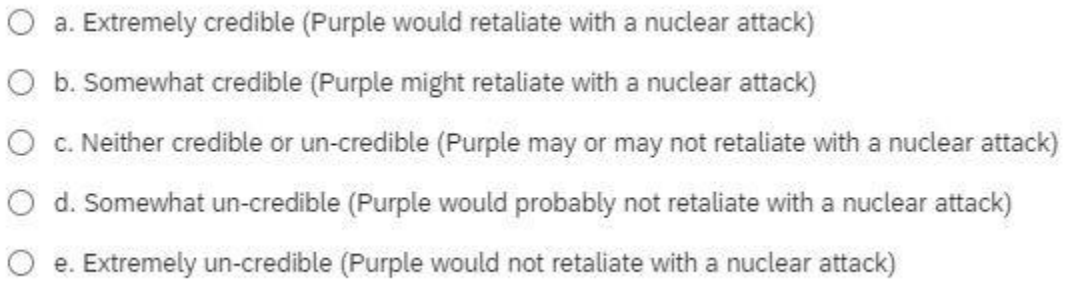


Figure 8 - Survey response options for attacks

5.1.2 Analysis and Results

As with the previous chapter, I will first briefly review my hypotheses and expected results based on the hypotheses. *H1: Entanglement deters attacks against NC3 space systems*. I expected that survey respondents with the entangled systems treatment would be less likely to conduct attacks against NC3 space systems than both their disentangled and unknown treatment counterparts. Additionally, the logic of this hypothesis suggests that responses to attacks against entangled and disentangled NC3 space systems should be more severe than unknown or disentangled conventional systems due to the critical role these systems play in strategic defense. *H2: Disentanglement of NC3 space systems makes attacks against conventional versions of the disentangled systems more likely.* Under this hypothesis, I expected survey respondents in the disentangled treatment to be more willing to attack conventional space systems and respond less severely to attacks against disentangled conventional systems.

The primary means of assessing my hypotheses with the elite survey was to look at variance in attacks against space systems based on treatment. This analysis finds no statistical significance among any treatment condition. I performed Chi-squared tests of independence as well as regressions for the independent variable (entanglement) and cannot reject the null hypotheses that entanglement status does not have an effect on the decision to attack space systems, broadly. Respondents in the disentangled treatment were far more likely to attack conventional systems compared to nuclear (21 attacks compared to 2) but were not more likely to conduct attacks overall than other entanglement treatments. .[339] With a relatively small sample size, differences between treatments would have needed to be much greater to make reasonable claims about the effect of treatment conditions on the decision to conduct attacks. On average, respondents in the unknown treatment were more likely to attack space systems, as would be expected based on the lack of awareness of NC3 system status. Surprisingly, however, respondents in the disentangled treatment were least likely to conduct attacks, which I will further explain using justifications provided by respondents in the qualitative section of this analysis. Below is an overview of the decision to attack space systems, by treatment.[340]

Table 28 - NC3 space system attack decisions by treatment

Treatment	Conducted Attacks	Did Not Conduct Attacks
Entangled (n = 19)	57.89% (n = 11)	42.11% (n = 8)
Disentangled (n = 19)	42.11% (n = 8)	57.89% (n = 11)
Unknown (n = 20)	65% (n = 13)	35% (n = 7)

[339] P-value for Chi-squared test was 0.34, and summary statistics can be viewed in Appendix 5.
[340] In addition to the three entanglement treatments, I also collected demographic data for elite participants, to include: NC3 experience, service, rank, age, and gender. On average, members of the Air Force, respondents with no NC3 experience, and females were more likely to support space system attacks, though with comparatively small sample sizes, no demographic factor had statistical significance.

Despite the inability to make claims about treatment effects based upon a direct measure of attacks, some useful inferences can still be made with the additional data collected. A closer look at what respondents chose to attack, how they conducted attacks, and why they chose not to attack provides greater insight into the effect of treatments on decision making.

The systems most commonly cited as being a source of inadvertent escalation as a result of entanglement are the early warning satellites that are used to detect missile launches and enable missile defense systems.[341] Respondents assigned significant escalation risk to attacks against these systems in both the entangled and disentangled treatments, and to some extent the unknown treatment as well. A number of respondents indicated that attacks against strategic missile warning systems would cross "red lines" and there were no attacks against strategic missile warning systems in both the entangled and disentangled treatments. One Space Force officer in the entangled treatment put it very simply, "I am avoiding targeting missile warning to avoid a nuclear escalation." Disentangled respondents conducted six attacks against conventional missile warning satellites and unknown status teams conducted four attacks, indicating that there is still a perceived military utility to such attacks, but the risk of escalation associated with strategic versions of these systems was too great.

In a similar vein, several respondents indicated in the feedback they provided that they perceived no such risk of nuclear escalation when attacking entangled/strategic ISR or SATCOM systems, particularly if non-kinetic weapons were used. In the words of one

[341] Acton, J. (2018); Arbatov, A., Dvorkin, V. and Topychkanov, P. (2017); Zhang, B. (2011); Zhao, T. and Bin, L. (2017)

Space Force officer, “Missile Warning serves a strategic function, so I would avoid destroying that target” but “ISR and SATCOM would be fair game for destruction because they are integral into Purple's power projection forward.” Another Air Force respondent echoed these sentiments and stated “Avoiding attacking Missile warning reduces chance of escalation. But attacking ISR and SATCOM capabilities allows for great surprise and freedom of movement and increases Purple’s fog of war.” These statements and actions provide interesting insight into the perceptions of attacking NC3 systems. It makes sense that not all NC3 systems would be viewed with the same level of criticality, but it is interesting that ISR and SATCOM systems appear to be widely regarded as safe and important targets among military space leaders. Despite the fictional scenario placing all of these systems on equal footing, respondents applied their own knowledge of NC3 systems and assigned a higher escalation risk to missile warning systems. Numbers in parenthesis represent attacks against strategic/nuclear systems.

Table 29 - NC3 space system attacks by treatment

Treatment	ISR	Missile Warning	SATCOM
Entangled	9	0	10
Disentangled	7 (0)	6 (0)	8 (2)
Unknown	12	4	8
Totals	**28 (0)**	**10 (0)**	**26 (2)**

In addition to the preference to avoid missile warning, there was a strong preference for non-kinetic attack options across all treatments. Only one respondent opted to use kinetic weapons, and this person was also one of the two respondents that attacked a disentangled nuclear system. The justification provided by the respondent for attacking nuclear systems with kinetic weapons was that the goal was to achieve “high efficacy” and that you “just have to deal with attribution, because there really is no low

attribution." This line of reasoning suggests that in the eyes of some participants, even systems that are clearly intended to support nuclear missions could be viable targets because an attacker cannot trust that these strategic systems wouldn't be used to augment the conventional versions of the systems during a conflict. However, the vast majority of participants viewed kinetic attacks as both dangerous for the space environment and unnecessary. This finding is in line with what CSIS and SWF found in their wargames with space elites, where only one kinetic space attack was conducted. As with wargaming participants, respondents preferred non-kinetic cyber attacks most, accounting for 59.38% of all attacks.

Table 30 - Types of attack conducted by treatment

Treatment	Kinetic Permanent	Non-Kinetic Permanent	Non-Kinetic Temporary	Permanent Cyber	Temporary Cyber
Entangled	0	0	5	2	4
Disentangled	1	1	2	1	3
Unknown	0	1	4	0	8
Totals	**1**	**2**	**11**	**3**	**15**

5.1.3 Other Findings

Perhaps the most interesting findings from the survey relate to how respondents perceived attacks against their own systems, as well as how they believed their attacks against adversary space systems would be perceived. In order to measure these perceptions, I asked respondents to assess what the most likely response would be to their attacks against their opponent's space systems. I assigned a value between 1 and 9 for the response options listed below and calculated mean scores for each of the treatments. Unsurprisingly, the highest scores (most severe responses) were in the disentangled nuclear treatment. Unlike the entangled and unknown treatments, attacks against these systems were unambiguously targeting Purple's NC3 capabilities, and as a result

respondents expected a harsher retaliation. It is interesting that respondents generally did not believe that any attacks would result in non-space military actions. It could be that the fictional states and capabilities involved did not generate the same level of impact that real attacks on real systems would, or it could also be that these respondents do not view attacks against space systems, even NC3 systems, as being particularly egregious or dangerous.

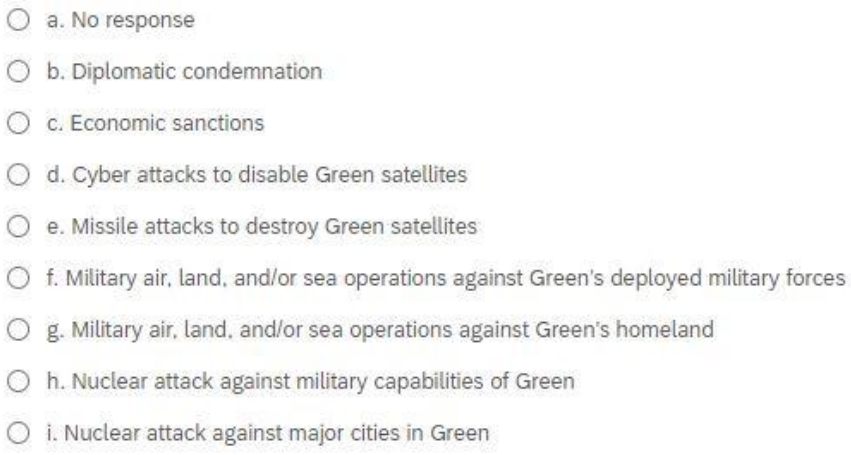


Figure 9 - Survey response options for attacks

Table 31 - Anticipated Purple responses to Green attacks

Treatment	Mean Response (Standard Error)	Standard Deviation	Median Response (Mode)
Entangled	4.05 (0.30)	1.32	4 (4)
Disentangled (Strategic/Nuclear)	4.84 (0.32)	1.42	5 (5)
Disentangled (Tactical/Conventional)	4.32 (0.28)	1.21	4 (4)
Unknown	4.05 (0.30)	1.36	4 (4)
Overall	4.31 (0.19)	1.41	4 (4)

Given the same input with the roles reversed, that is with Purple attacking Green's systems, respondents viewed the same attacks as more serious and responded

accordingly. International relations theory provides some explanation for why this might be the case. States tend to view their own actions as being less hostile than the same actions by their competitors or adversaries.[342] Jervis has written about this tendency as it relates to the security dilemma and claims that "states underestimate the degree to which they menace others."[343] This awareness predates Jervis though, and Edward Grey wrote about this tendency nearly 100 years ago. He wrote: "neither party can see the nature of the predicament he is in, for each only imagines that the other party is being hostile and unreasonable."[344] These statements could help to explain why respondents view the same input so differently based only upon whether they were the attacker or the victim, but there are also other, possibly better explanations that relate to human nature.

Behavioral economists Daniel Kahneman and Amos Tversky offer a possible explanation with prospect theory, specifically loss aversion. Put simply, "the response to losses is more extreme than the response to gains."[345] Humans tend to view losses as more impactful than gains of equal measure; "losing ten dollars, for example, annoys us more than gaining ten dollars gratifies us."[346] Robert Jervis has done extensive work applying prospect theory to international relations and asserts that "because people are willing to take unusual risks to recoup recent losses…a decision-maker might risk costly escalation or even world war if such a move held out the prospect of reversing a defeat."[347] Building upon the tenets from the previous paragraph, "When states overestimate others' hostility, as they frequently do, they will expect losses unless they

[342] Jervis, R. (1976), 70-72.
[343] Jervis, R. (1978), 200.
[344] Grey, E. (1925), 91.
[345] Tversky, A. and Kahneman, D. (1986), 258.
[346] Jervis, R. (1995), 187.
[347] Jervis, R. (1995), 197.

take strong if not aggressive action."[348] While these explanations and findings do not specifically address willingness to attack NC3 space systems, they do raise significant questions about prospect theory and decision making that should be explored with future research. The table below shows mean responses for attacks against Green's space systems (respondents are the victim state in this case).

Table 32 - Green Responses to Purple Attacks

Treatment	Mean Response (Standard Error)	Standard Deviation	Median Response (Mode)
Entangled	5.05 (0.20)	0.89	5 (6)
Disentangled (Strategic/Nuclear)	5.68 (0.40)	1.75	5 (5)
Disentangled (Tactical/Conventional)	4.79 (0.27)	1.19	5 (5)
Unknown	4.75 (0.25)	1.13	5 (6)
Overall	5.16 (0.17)	1.36	5 (5)

A comparison between the two sets of responses is provided in Table 34, below. For the entangled treatment, responses were a full point higher when respondents were the victim state versus the attacking state. Overall, the mean and median responses jumped from 4 to 5 as well. Going back to the original question of whether respondents in each treatment would conduct attacks, it makes sense that disentangled teams had higher mean scores on average, as fewer of those respondents conducted attacks, indicating they believed the consequences outweighed the benefits. Unknown status respondents had lower average scores, which also makes sense because they had the highest number of attacks. The willingness to attack space systems is largely influenced

[348] Jervis, R. (1995), 192.

by the expected cost of those attacks in terms of retaliation, so it is interesting to see that logic play out in these questions as well.

Table 33 - Comparison of Responses to Attacks

Treatment	Mean Response Purple Attacked (Median)	Mean Response Green Attacked (Median)	Deltas
Entangled	4.05 (4)	5.05 (5)	1.00 (1)
Disentangled (Strategic/Nuclear)	4.84 (5)	5.68 (5)	0.84 (0)
Disentangled (Tactical/Conventional)	4.32 (4)	4.79 (5)	0.47 (1)
Unknown	4.05 (4)	4.75 (5)	0.70 (1)
Overall	4.31 (4)	5.16 (5)	0.85 (1)

In the previous few paragraphs, I discussed what respondents believed the most *likely* response would be to attacks against NC3 space systems. For the next set of data, I asked respondents to consider the most *dangerous* response. As I discussed in Chapter 2, the U.S. maintains the position that attacks against NC3 systems could be met with nuclear retaliation.[349] Though there is no consensus on whether this threat of nuclear retaliation is likely to occur, there is at least the perception in the U.S, China, and Russia that it is possible.[350] Again, this is a threat that leaves something to chance.[351] To gain better insight into whether or not this threat is perceived to be credible, I asked participants to assess how credible Purple's threat of nuclear retaliation was in response

[349] Office of the Secretary of Defense. (2018), 21.
[350] Arbatov, A., Dvorkin, V., and Topychkanov, P. (2017); Zhao, T. and Bin, L. (2017)
[351] Schelling, T. (1966)

to attacks against their NC3 space systems.[352] This question complements the credibility question from the wargames. Respondents selected from the following options:

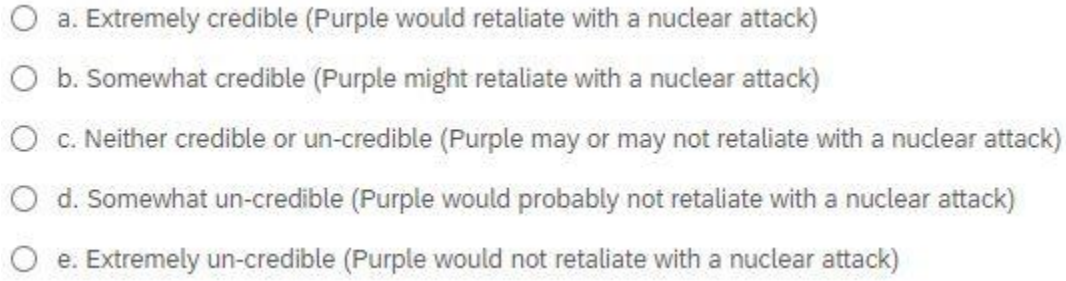


Figure 10 - Survey response options for credibility

Table 34 - Credibility responses by treatment

Treatment	Mean Response (Standard Error)	Standard Deviation	Median Response (Mode)
Entangled	3.68 (0.21)	0.92	4 (4)
Disentangled (Strategic/Nuclear)	3.42 (0.29)	1.27	4 (4)
Unknown	3 (0.26)	1.18	3 (2)
Overall	3.36 (0.15)	1.17	4 (4)

Across all treatments, respondents viewed nuclear retaliation to be between "neither credible or un-credible" and "somewhat un-credible." There are some important takeaways from these responses. First, only 9 of 58 (15.52%) respondents believed nuclear retaliation was extremely un-credible, and these were evenly distributed among treatments. The vast majority of respondents (84.48%) found the threat to at least be possible, with 15 of 58 (25.85%) believing the threat to be either somewhat or extremely credible. While only 3 of 58 (5.17%) respondents believed nuclear retaliation was the most *likely* response to attacks against NC3 space systems, the possibility of such a

[352] Participants in the unknown treatment condition were unaware of NC3 system status, so they received a generic version of this question that asked how credible is it for a state to threaten nuclear retaliation in response to attacks against their space systems.

response is widely acknowledged with these findings. Although the question of credibility was not framed the same way between experiments, when compared to wargaming participants, of whom over 70% found the threat of nuclear retaliation to be credible, the lower scores for credibility in the elite surveys could explain why entanglement was less clearly associated with deterrence in the surveys. When participants believed that attacks against entangled or disentangled nuclear systems could be met with nuclear retaliation, they were more likely to be deterred from attacking those systems. If participants did not find the threat of nuclear retaliation credible, they were less likely to be deterred. This seems logical, but it is important to point out that underlying my theory is an assumption that the threat of severe retaliation in response to attacks against NC3 space systems is perceived by potential attackers as credible. This is a possible alternative explanation for why entanglement treatment was not statistically significant for the elite surveys.

The final data I gathered from respondents were qualitative justifications for decisions to attack or not attack space systems. For the 26 respondents who chose not to attack space systems, the justifications varied. Respondents in the entanglement treatment that chose not to attack space systems overwhelmingly cited risks of escalation as justification, as would be expected. According to one respondent in this treatment "attacking Purple's space assets risks an unnecessary and possibly dangerous escalation in conflict." Responses in the other treatments were more varied. A couple of respondents in the disentangled treatment cited limited military value for attacks. These justifications speak to the potential deterrence by denial benefits of resilient architectures, though resilience was an assumption on the part of the respondents, rather than a variable

introduced in the background materials. One respondent said "they [Purple] have a lot of ways to pass information," so they did not believe these attacks would actually limit the ability of a state to conduct operations in a meaningful way. Several respondents cited the high likelihood of attacks being attributed as being the primary motivation not to attack. Others mentioned that it was unnecessary to attack assets in the space domain to achieve their objectives, and that it was important to "avoid conflict that extends to space." The table below categorizes the justifications provided by respondents who chose not to attack NC3 space systems.

Table 35 - Justifications for not attacking NC3 space systems

Justification	Entangled	Disentangled	Unknown
Risk of Undesired/Uncontrolled Escalation	6	2	2
Limit attacks to terrestrial domain (preserve space)	0	3	3
Risk of attribution is too high	1	3	2
Limited military value	0	2	0
Signals vulnerabilities to adversary	0	1	0
No response given	1	0	0

For respondents that did attack space systems, the primary justification for conducting the attacks was to achieve military objectives. There were no other reasons cited to attack an opponent's space systems other than to enable mission success. However, respondents did provide some useful information on why they chose to attack the systems they did, and why they selected the weapons they did. The table below captures the reasoning of respondents who chose to attack space systems. Again, responses were varied, though a few were common across treatments. Overall, respondents believed it was safe to attack ISR and SATCOM systems, particularly if non-kinetic weapons were used. According to one respondent in the entanglement treatment, non-kinetic weapons can be employed without "compelling a robust military response."

Another respondent in the unknown treatment wrote that "non-kinetic attacks that are temporary, if done with the correct timing and tempo and in conjunction with the rest of the operations, can be a significant advantage against a peer."

Table 36 - Justifications for types of attack on NC3 space systems

Justification	Entangled	Disentangled	Unknown
Temporary/non-kinetic attacks are safe/effective	1	0	6
Attacking ISR/SATCOM will not cause escalation, avoid missile warning	4	2	1
Conventional targets avoid escalation	0	5	0
Safe to target anything but nuclear/NC3, avoid missile warning	3	0	3
Avoid debris creation	0	0	2
Manage escalation better with high-probability attacks	0	0	1
Have to target all assets to achieve effects	0	1	0
Easy to jam systems without high-level approvals	1	0	0
No response given	2	0	0

5.1.4 Elite Survey Summary

Ultimately the elite survey failed to yield statistically significant evidence of the effects of entanglement on deterrence, at least not broadly applied. Entanglement appears only to have deterred attacks against missile warning systems for these military space security elites. No attacks were conducted against entangled missile warning systems, or the strategic/nuclear versions of the disentangled missile warning systems, and respondent feedback cited a much greater risk of escalation with these systems. Entangled respondents cited escalation as the primary factor for not attacking space systems, which would also be expected, but over half of entangled respondents still conducted attacks. Like the wargames, non-kinetic attacks were again the preferred choice, with cyber taking precedence in that group.

One of the more interesting findings from the elite surveys was that respondents perceived the same attacks differently based on whether they were the attacker or victim,

and this applied across entanglement treatments. This disparity could signal a dangerous misperception that affects decisions of whether or not to attack space systems. Attacking states might conduct cost-benefit analyses based on expected consequences that are significantly lower than actual consequences might be. Finally, though not the most likely response in the eyes of respondents, the threat of nuclear retaliation in response to attacks against NC3 space systems was viewed as possible by a majority.

I was surprised by all of the findings from the elite survey, and the lack of correlation or causal relationship between treatments and the decision to attack space systems could challenge the validity of my theory. However, there are some possible explanations for why respondents behaved in the manner in which they did. Some respondents in each of the treatments behaved exactly as I would have expected, with some entangled respondents declining to attack due to the risk of massive retaliation, and some disentangled respondents finding attacks against conventional systems to be safe alternatives. However, these perspectives were not widely shared enough to make claims about deterrence through entanglement in this experiment. It is possible that for military space elites, my theory applies only to missile warning systems. It is also possible that the tendency of military members to recommend more hawkish approaches in general led more respondents to support attacks, regardless of treatment. Future research should compare the responses of military space elites with space elites from other institutions like academia, think tanks, or diplomacy-oriented organizations. The role of the military is to provide options to civilian decision makers regarding the use of force, so perhaps respondents who supported attacks did so with that purpose in mind. It is also possible that entanglement simply does not outweigh perceived military utility, even if the

consequences of attacks are expected to be severe. Whatever the reason, I cannot claim that deterrence through entanglement best explains the decisions of these elite respondents, though the data are nevertheless useful for expanding the current body of knowledge of space security.

5.2 Public Opinion Survey

5.2.1 Public Opinion Survey Design and Implementation

In addition to the elite survey, I fielded a public survey to gauge perceptions about space system attacks and what response options the public would support. To test the survey design and execution, I initially recruited 50 respondents through Amazon's Mechanical Turk (MTurk) platform, and again used Qualtrics to host the survey. Based on the feedback from this initial survey, I determined that the existing three treatment conditions needed to be expanded to allow for greater fidelity in the responses. In the initial version of the survey, I told respondents that "A rival country has attacked U.S. military satellites that are used for intelligence collection and communications." I then added the treatment conditions following this statement. However, respondent feedback suggested that it was too difficult to respond to survey questions without knowing what type of attack occurred. In the second trial run, I included both kinetic and non-kinetic attacks in each of the treatment conditions and specified the type of weapon with which the attack was conducted. The updated statements were: "A rival country launched a missile attack that destroyed U.S. intelligence and communications satellites" and "A rival country conducted a cyber attack that disabled U.S. intelligence and communications satellites."

Following these statements, I added information related to the treatment conditions. Entangled respondents were told: “These satellites are also used for nuclear command and control, which enables detection and defense against nuclear attacks against the U.S.” Respondents that were assigned to the strategic/nuclear disentangled group received a similar statement which was: “These satellites are used for nuclear command and control, which enables detection and defense against nuclear attacks against the U.S.” Respondents in the tactical/conventional disentangled group were told “These satellites are used for tactical missions only and ARE NOT used for nuclear command and control.” Because this survey asked participants to respond to an attack rather than choosing whether or not to conduct an attack, and had standardized response options, I had to have two disentangled treatment groups (strategic/nuclear, and tactical/conventional), unlike the elite survey and wargames. Respondents in the unknown treatment received no additional information. These statements had to be as clear and concise as possible to enable participants to answer effectively with little to know knowledge of space, which is a limitation of conducting a public survey about a complex topic.

During a second trial run of 300 respondents, I discovered that less than 40% of respondents passed the treatment check, which was no better than random chance for the three-question validation. As a result, I instituted additional measures to improve the quality of responses. First, I added a second validation question that required participants to read a sentence and select the response “I have a question” in order to proceed; the other options were “I understand” and “I do not understand.” Any respondent that selected something other than “I have a question” was sent to the end of the survey and

not provided a completion code, which would have otherwise counted against my sample. This measure alone eliminated 187 of 817 survey respondents. Additionally, I randomized the order of the treatment check responses to reduce the number of participants who simply selected the first option. Finally, I added more stringent requirements to the MTurk workers who were able to participate. In addition to the existing criteria of being in the U.S. and being over the age of 18, I also required over 100 approved tasks with over a 98% approval rate. Finally, I added a statement in my survey that failure to pass the validation checks could result in a rejected task, which hurts the MTurk workers' ability to participate in future tasks. With these modifications, I was able to obtain an 80% pass rate (which was higher than the elite sample), reduce the deviation/error within treatments and improve my confidence in the validity and quality of the responses.

Following the validation steps and background information, respondents were asked to answer the following question, which was coded using the same 1-9 scale of severity as the elite sample. I also asked respondents to provide a sentence or two explaining their reasoning and conducted an additional validation question to assess their understanding of the treatment condition to which they were assigned.

Figure 11 - Public survey question and response options

Finally, respondents provided basic demographic information including age, gender identity, race/ethnicity, level of education, political views, veteran status, and income. A summary of how the respondents in my survey compare to national averages is provided below. In general, my sample was overrepresented in males, whites, college graduates, and military veterans compared to national averages. Additionally, a higher percentage of survey respondents were liberal (45.16%) in their political beliefs than conservative (29.24%), however, there was little statistically significant correlation between political beliefs and response. Based on previous research in IR, I expected conservatives to favor more hawkish or severe retaliatory measures than liberal respondents, but responses were relatively similar across the political spectrum, with conservatives scoring an average of 4.18, liberals 4.03, and moderates 3.87. The only differences with any statistical significance were among people who identified as “very conservative” within the non-kinetic treatment, who averaged a little over half a point higher than those that identified as “very liberal.” However, respondents who identified as “liberal” and “conservative” had roughly equal responses, and moderates scored

lowest of all groups within the non-kinetic treatment. In the kinetic treatment, however moderates scored over half a point higher than liberals, though the very conservative groups still scored highest of all. I also expected military veterans to score slightly higher in response severity, but again, the differences were present but only statistically significant within the non-kinetic treatment, where veterans averaged over half a point higher than non-veterans. In the kinetic treatment, however, veterans scored lower than non-veterans. Overall, veterans averaged 4.26 compared to non-veterans at 4.02.[353]

[353] Statistical summaries for these and all other variables are available in Appendix 5.

Table 37 - Demographic information for public survey respondents

Category	Public Sample Survey	National Sample[354]
Gender		
Male	59.07%	49.24%
Female	40.73%	50.76%
Race		
White Alone	73.79%	61.63%
Black or African American Alone	4.84%	12.40%
American Indian or Alaska Native Alone	0.60%	1.12%
Native Hawaiian and Other Pacific Islander Alone	0.00%	0.21%
Asian Alone	9.07%	6%
Hispanic	8.27%	18.73%
Mixed Races	9.68%	10.21%
Other	0.60%	8.40%
Median Age	37.0	38.2
Educational Attainment		
High School Incomplete	2.82%	11.47%
High School Graduate, GED, or Equivalent	5.44%	26.67%
Some College	14.92%	20.30%
Associate Degree	9.07%	8.64%
Bachelor's Degree	58.63%	20.21%
Some Postgraduate, or Professional Degree	13.71%	12.71%
Income		
Less than $10,000	4.84%	5.80%
$10,000-$24,999	8.47%	12.60%
$25,000-$49,999	31.65%	20.60%
$50,000-$74,999	28.23%	17.20%
$75,000 or more	26.61%	43.80%
Military Veteran		
Yes	25.58%	7.10%
No	75.81%	92.90%
Political Views		
Very Liberal	13.51%	
Liberal	31.65%	
Moderate	25.20%	
Conservative	18.35%	
Very Conservative	10.89%	

[354] United States Census Bureau, (2020)

5.2.2 Analysis and Results

Public opinion can be important for constraining or emboldening decision makers who would be charged with responding to attacks against space systems, so gauging public perceptions about these attacks contributes an additional layer of understanding to my research. While it is difficult for the general public to conceptualize the impact of attacks against NC3 space systems, the inputs provided mirror the type of information they would receive in a real-world situation in which news reports provide a glimpse into what has occurred, and public opinion can ultimately shape how states respond, whether or not those opinions are formed with deep understanding of the situation. Using the logic of my theory, I expect that respondents in the entangled treatment would support more severe response measures than those in the disentangled conventional/tactical treatment. Additionally, based on the results of the wargames and elite surveys, I also expect respondents to support more severe retaliation when kinetic weapons are employed by the adversary, versus non-kinetic. In order to quantitatively assess the effects of treatments, I again used the 1-9 scale for response options. Using these numerical responses as the DV, I performed Chi-square tests of independence for the independent variable (entanglement), as well as regressions for the IV and each of the other categorical data sets within the demographic information.

As with the elite survey, the relationship between entanglement treatment and response was not statistically significant, though there are some interesting trends when looking at averages.[355] The table below provides the mean responses by treatment, and as expected, the entangled treatment had the highest average response, though with such

[355] P-value for Chi-squared test based on treatment was 0.09, ANOVA p-value for the kinetic group was 0.19, and for the non-kinetic group ANOVA p-value was 0.65.

high variance within treatments it was not different enough from other treatments to make strong claims about the effect of entanglement. What seems to be clearer is that respondents favored more severe retaliation in response to attacks on strategic/nuclear disentangled systems than the tactical/conventional versions of those systems, with median and mode responses a full point lower for the latter group. This finding is consistent throughout my research; attacks against conventional systems are not viewed with the same level of severity as attacks against nuclear systems. While this is logical, it is nevertheless useful to see this perspective play out across each experimental approach.

The qualitative data collected from respondents also helps to clarify the response scores. The primary justification provided by respondents across treatments was that they chose an option that was proportional to the initial attack, or "eye for an eye" as many put it. The input for the kinetic attack was that a rival state conducted a missile attack that destroyed U.S. satellites, so it makes sense that the median and mode responses for all but the disentangled tactical category were 5, which corresponds to a retaliatory missile attack on rival satellites.

Table 38 - Responses to kinetic attacks by treatment

Treatment	Mean Response (Standard Error)	Standard Deviation	Median Response (Mode)
Entangled	4.61 (0.18)	1.55	5 (5)
Disentangled (Strategic/Nuclear)	4.49 (0.18)	1.46	5 (5)
Disentangled (Tactical/Conventional)	4.04 (0.21)	1.53	4 (4)
Unknown	4.48 (0.19)	1.31	5 (5)
Overall	4.43 (0.10)	1.48	4 (5)

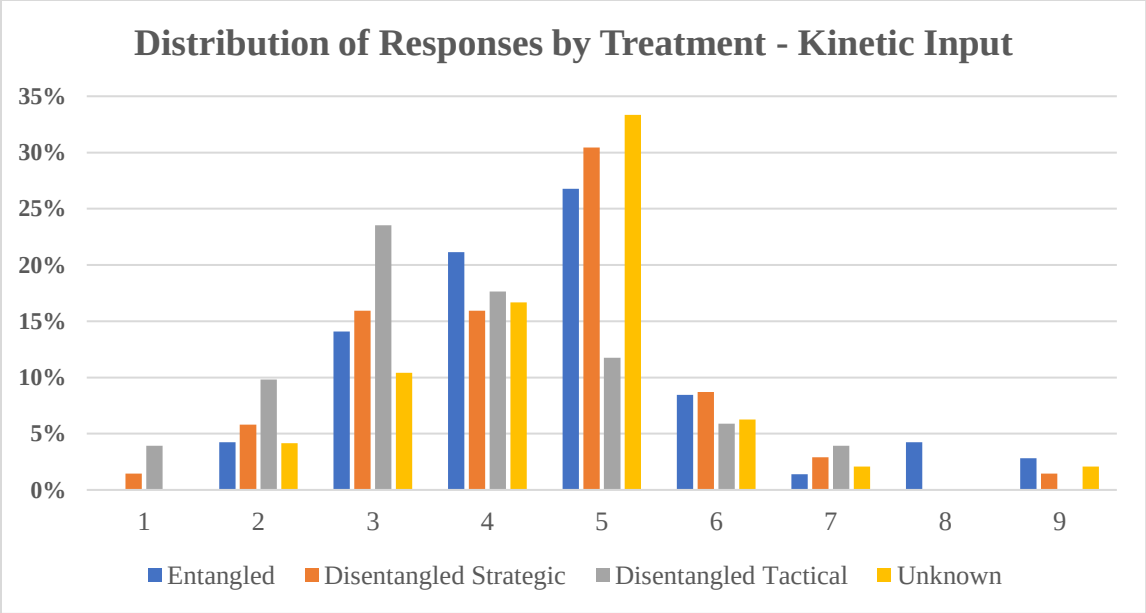


Figure 12 - Distribution of responses to kinetic attack by treatment

Carrying this logic forward, respondents who received the input that a non-kinetic cyber attack disabled satellites also tended to favor a non-kinetic cyber counter attack. The median and mode responses for all but the entangled treatment was 4, which again corresponds to a cyber attack against rival satellites. Here too, there is a difference in response between strategic and tactical disentangled systems, though with the non-kinetic attack, the gap is much smaller. The key takeaway from these data is that the differences between treatments are not statistically significant, but the mean responses between kinetic and non-kinetic groups are. In fact, this was the only statistically significant factor for the public surveys.[356] The table below shows mean responses by treatment for the non-kinetic attack group, and the chart depicts the distribution of responses by treatment.

[356] P-value for regression of kinetic vs. non-kinetic is 0.0014.

Table 39 - Responses to non-kinetic attacks by treatment

Treatment	Mean Response (Standard Error)	Standard Deviation	Median Response (Mode)
Entangled	3.74 (0.15)	1.27	4 (3)
Disentangled (Strategic/Nuclear)	3.75 (0.18)	1.50	4 (4)
Disentangled (Tactical/Conventional)	3.51 (0.17)	1.32	4 (4)
Unknown	3.80 (0.15)	1.17	4 (4)
Overall	3.70 (0.08)	1.33	4 (4)

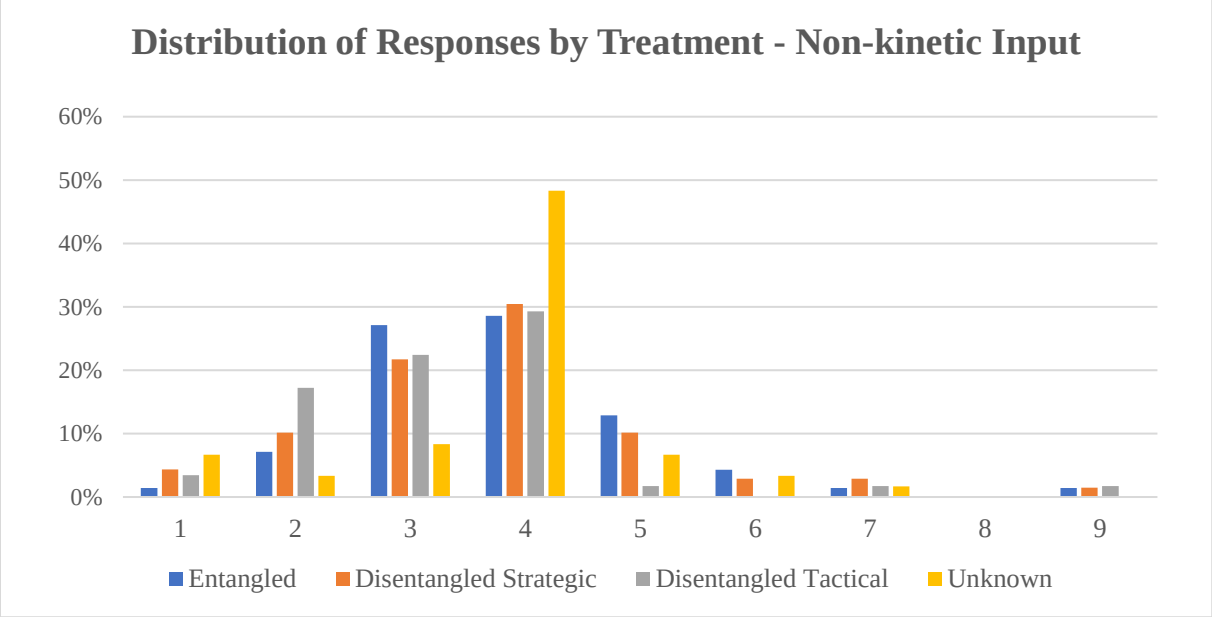


Figure 13 - Distribution of responses to non-kinetic attack by treatment

Mean responses were significantly higher for kinetic versus non-kinetic attack inputs, and this was particularly pronounced for the entangled treatment. For all but the disentangled tactical treatment, median responses were a point higher for kinetic versus non-kinetic attacks. This seems logical, as the permanent destructive nature of kinetic attacks is much more severe than non-kinetic attacks, but the data are nevertheless interesting to demonstrate that public opinion aligns with these expectations. These

results also give me confidence that respondents in this survey actually read and understood the inputs they received. The table and chart below provide comparisons between mean responses for the kinetic and non-kinetic groups.

Table 40 - Comparison of responses to kinetic and non-kinetic attacks

Treatment	Mean Response Kinetic Attack (Median)	Mean Response Non-kinetic Attack (Median)	Deltas
Entangled	4.61 (5)	3.74 (4)	0.87 (1)
Disentangled (Strategic/Nuclear)	4.49 (5)	3.75 (4)	0.74 (1)
Disentangled (Tactical/Conventional)	4.04 (4)	3.51 (4)	0.53 (0)
Unknown	4.48 (5)	3.80 (4)	0.68 (1)
Overall	4.43 (4)	3.70 (4)	0.73 (0)

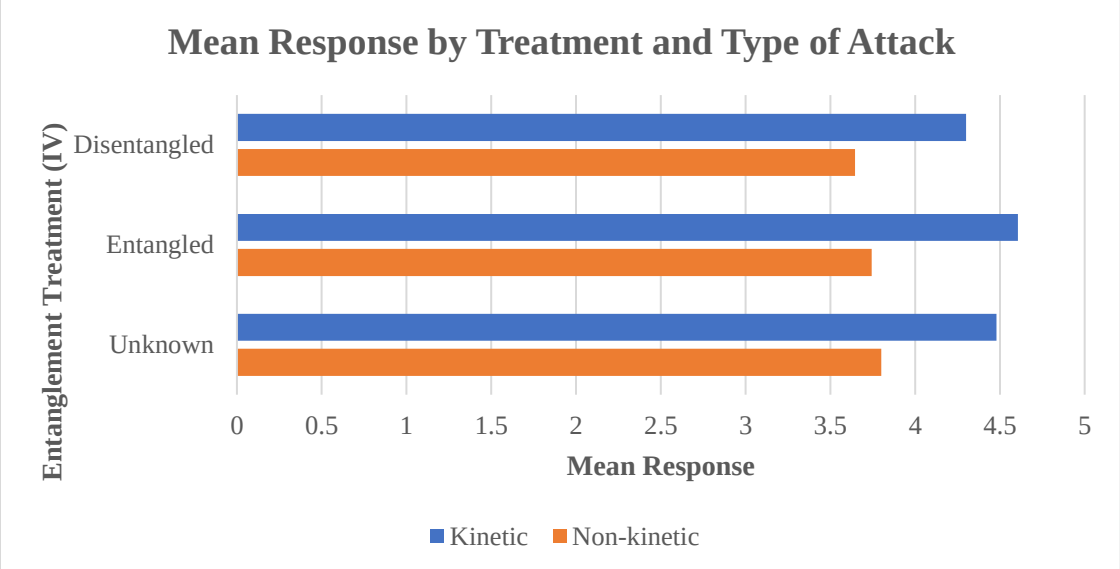


Figure 14 - Comparison of responses to non-kinetic attack by treatment

Table 41 - Responses to attacks by treatment

Response Option	Kinetic (n = 239)	Non-Kinetic (n = 257)	Overall (n = 496)
1. No response	1.26% (n = 3)	4.28% (n = 11)	2.82% (n = 14)
2. Diplomatic condemnation	6.69% (n = 16)	11.67% (n = 30)	9.27% (n =46)
3. Economic sanctions	20.08% (n = 48)	23.74% (n = 61)	21.98% (n = 109)
4. Cyber attacks to disable rival satellites	22.59% (n = 54)	42.41% (n = 109)	32.86% (n = 163)
5. Missile attacks to destroy rival satellites	32.22% (n = 77)	10.89% (n = 28)	21.17% (n = 105)
6. Military air, land, and/or sea operations against rival's deployed military forces	9.21% (n = 22)	3.89% (n = 10)	6.45% (n = 32)
7. Military air, land, and/or sea operations against rival's homeland	4.18% (n = 10)	1.56% (n = 4)	2.82% (n = 14)
8. Nuclear attack against military capabilities of rival country	2.09% (n = 5)	0.39% (n = 1)	1.21% (n = 6)
9. Nuclear attack against major cities in rival country	1.67% (n = 4)	1.17% (n = 3)	1.41% (n = 7)

While these findings do not directly answer my hypotheses, it does appear that attacks against disentangled conventional systems are perceived as the least serious of all and generate the lowest mean responses. Not only could adversaries believe these attacks are less severe, they could also take some comfort in knowing public opinion supports a lower level of retaliation, compared to other treatments. Respondents in the entangled treatment had the highest average score, but it is not significantly high enough to claim that entanglement alone is responsible for the increased score. Entangled respondents were the least likely to take no action and were most likely to recommend nuclear retaliation, so there is some expectation of a harsher response for entangled systems, as would be expected with my theory. The table and graph below provide mean scores and distribution of responses by treatment, irrespective of whether the attack was kinetic or non-kinetic.

Table 42 - Overall responses to attacks by treatment

Treatment	Mean Response (Standard Error)	Standard Deviation	Median Response (Mode)
Entangled	4.18 (0.12)	1.48	4 (4)
Disentangled (Strategic/Nuclear)	4.12 (0.13)	1.52	4 (4)
Disentangled (Tactical/Conventional)	3.76 (0.13)	1.45	4 (4)
Unknown	4.10 (0.12)	1.28	4 (4)
Overall	3.70 (0.08)	1.33	4 (4)

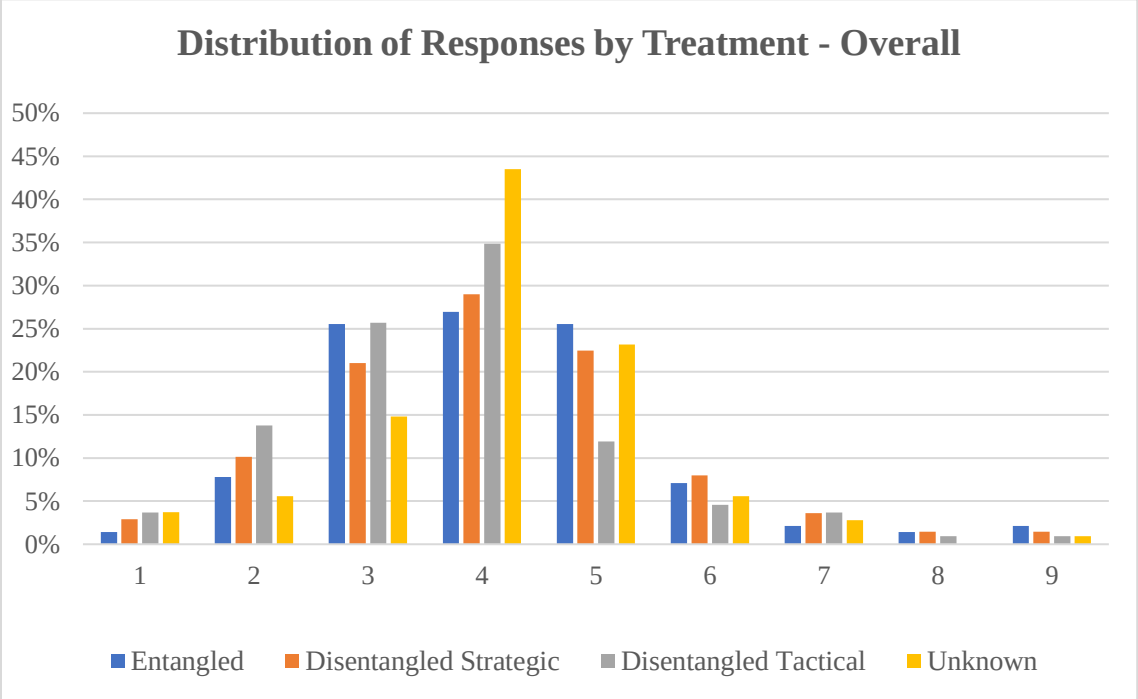


Figure 15 - Overall distribution of responses to attacks by treatment

Table 43 - Overall responses by treatment

Response Option	Entangled (n = 141)	Disentangled Strategic (n = 138)	Disentangled Tactical (n = 109)	Unknown (n = 108)
1. No response	1.42% (n = 2)	2.90% (n = 4)	3.67% (n = 4)	3.70% (n = 4)
2. Diplomatic condemnation	7.80% (n = 11)	10.14% (n = 14)	13.76% (n = 15)	5.56% (n = 6)
3. Economic sanctions	25.53% (n = 36)	21.01% (n = 29)	25.69% (n = 28_	14.81% (n = 16)
4. Cyber attacks to disable rival satellites	26.95% (n = 38)	28.99% (n = 40)	34.86% (n = 38)	43.52% (n = 47)
5. Missile attacks to destroy rival satellites	25.53% (n = 36)	22.46% (n = 31)	11.93% (n = 13)	23.15% (n = 25)
6. Military air, land, and/or sea operations against rival's deployed military forces	7.09% (n = 10)	7.97% (n = 11)	4.59% (n = 5)	5.56% (n = 6)
7. Military air, land, and/or sea operations against rival's homeland	2.13% (n = 3)	3.62% (n = 5)	3.67% (n = 4)	2.78% (n = 3)
8. Nuclear attack against military capabilities of rival country	1.42% (n = 2)	1.45% (n = 2)	0.92% (n = 1)	0.00% (n = 0)
9. Nuclear attack against major cities in rival country	2.13% (n = 3)	1.45% (n = 2)	0.92% (n = 1)	0.93% (n = 1)

In addition to selecting from the nine response options, survey participants also provided justifications for their responses. These justifications varied greatly, but there are some trends both in general and by treatment. Overall, the most common justification was that the response selected was proportional. Over a quarter of respondents selected options that they believed matched the initial attack, and this was the most common reason provided across all treatments and types of attack. Interestingly, in the kinetic attack category, for both the entangled and disentangled strategic treatments, the second most common justification was that the option chosen needed to be a strong response or decisive action. Many of these respondents said things like "such an attack must be met with swift and decisive reprisal" or "we are now in a weakened position so a posture of strength and showing no fear would be important." For the disentangled tactical and

unknown treatments in the kinetic category, the second most common justification focused on the benefits of economic sanctions. Respondents in this group said things like "[economic sanctions] would be the most ethical way that will punish but does no physical harm to our environment and citizens" and "sanctions would provide an avenue for negotiations." Based on these justifications, respondents clearly perceived entangled and disentangled nuclear systems as warranting a more intense response.

For respondents who faced non-kinetic attacks, proportional response was still the primary justification given, however, soft power justifications gained traction. Respondents in the non-kinetic group were twice as likely to cite the need for diplomacy as a justification and almost half as likely to extol decisive action. Economic justifications also became more prevalent in all but the unknown treatment group. Like the wargames and elite surveys, respondents across treatments perceived cyber attacks to be both useful and relatively safe. If there is one common theme across all of my research findings, it is that cyber attacks have become expected in modern conflict, and many people view cyber attacks more as a tool of diplomacy than an instrument of military power. While 20% of respondents did not answer or provided unusable or unintelligible answers, the quantity and quality of the other justifications improves my confidence in the validity of these findings.

Table 44 - Justifications for responses to kinetic attacks by treatment

Justification	Entangled (n = 71)	Disentangled Strategic (n = 69)	Disentangled Tactical (n = 51)	Unknown (n = 48)	Totals (n = 239)
Proportional Response/avoid further escalation	23.94% (n = 17)	26.09% (n = 18)	23.53% (n = 12)	29.17% (n = 14)	25.52% (n = 61)
No response given/Unintelligible	25.35% (n = 18)	24.64% (n = 17)	7.84% (n = 4)	22.92% (n = 11)	20.92% (n = 50)
Decisive/strong response, show of force	18.31% (n = 13)	17.39% (n = 12)	9.80% (n = 5)	14.58% (n = 7)	15.48% (n = 37)
Economic sanctions are effective	5.63% (n = 4)	7.25% (n = 5)	17.65% (n = 9)	14.58% (n = 7)	10.46% (n = 25)
Cyber attacks are safe/effective	7.04% (n = 5)	10.14% (n = 7)	13.73% (n = 7)	8.33% (n = 4)	9.62% (n = 23)
Deter/Defend against future attacks	9.86% (n = 7)	4.35% (n = 3)	1.96% (n= 1)	2.08% (n = 1)	5.02% (n = 12)
Unnecessary to use force/diplomacy first	1.41% (n = 1)	4.35% (n = 3)	9.80% (n = 5)	4.17% (n = 2)	4.60% (n = 11)
Do not support war/violence	4.23% (n = 3)	2.90% (n = 2)	1.96% (n= 1)	4.17% (n = 2)	3.35% (n = 8)
Send warning to adversary	0% (n = 0)	0% (n = 0)	5.88% (n = 3)	0% (n = 0)	1.26% (n = 3)
Unnecessary to take action	0% (n = 0)	0% (n = 0)	5.88% (n = 3)	0% (n = 0)	1.26% (n = 3)
Avoid loss of life	1.41% (n = 1)	1.45% (n = 1)	1.96% (n= 1)	0% (n = 0)	1.26% (n = 3)
Consistent with policy	1.41% (n = 1)	0% (n = 0)	0% (n = 0)	0% (n = 0)	0.42% (n = 1)
Limit debris creation	1.41% (n = 1)	0% (n = 0)	0% (n = 0)	0% (n = 0)	0.42% (n = 1)
Recoup damages	0% (n = 0)	1.45% (n = 1)	0% (n = 0)	0% (n = 0)	0.42% (n = 1)

Table 45 - Justifications for responses to non-kinetic attacks by treatment

Justification	Entangled (n = 70)	Disentangled Strategic (n = 69)	Disentangled Tactical (n = 58)	Unknown (n = 60)	Totals (n = 257)
Proportional Response/avoid further escalation	32.86% (n = 23)	24.64% (n = 17)	29.31% (n = 17)	45% (n = 27)	32.68% (n = 84)
Economic sanctions are effective	17.14% (n = 12)	24.64% (n = 17)	18.97% (n = 11)	6.67% (n = 4)	17.12% (n = 44)
No response given/Unintelligible	17.14% (n = 12)	15.94% (n = 11)	3.44% (n = 2)	8.33% (n = 5)	11.67% (n = 30)
Unnecessary to use force/diplomacy first	8.57% (n = 6)	5.80% (n = 4)	17.24% (n = 10)	10% (n = 6)	10.12% (n = 26)
Decisive/strong response, show of force	10% (n = 7)	5.80% (n = 4)	12.07% (n = 7)	6.67% (n = 4)	8.56% (n = 22)
Cyber attacks are safe/effective	4.29% (n = 3)	7.25% (n = 5)	10.34% (n = 6)	11.67% (n = 7)	8.17% (n = 21)
Deter/Defend against future attacks	2.86% (n = 2)	7.25% (n = 5)	3.44% (n = 2)	8.33% (n = 5)	5.45% (n = 14)
Unnecessary to take action	0% (n = 0)	1.45% (n = 1)	3.44% (n = 2)	3.33% (n = 2)	1.94% (n = 5)
Do not support war/violence	0% (n = 0)	5.80% (n = 4)	1.72% (n = 1)	0% (n = 0)	1.94% (n = 5)
Avoid loss of life	2.86% (n = 2)	0% (n = 0)	0% (n = 0)	0% (n = 0)	0.78% (n = 2)
Test adversary intentions/commitment	1.43% (n = 1)	1.45% (n = 1)	0% (n = 0)	0% (n = 0)	0.78% (n = 2)
Easiest to accomplish	1.43% (n = 1)	0% (n = 0)	0% (n = 0)	0% (n = 0)	0.39% (n = 1)
Send warning to adversary	1.43% (n = 1)	0% (n = 0)	0% (n = 0)	0% (n = 0)	0.39% (n = 1)

5.3 Constraints and Limitations

There are a number of limitations that are at play with both surveys. The most significant limitation of the elite survey is the relatively small number of respondents, as well as the concentration of these respondents in the FGO ranks. While this was the target demographic based on the role the survey asks respondents to play, ultimately more senior leaders (both military and civilian) would be called upon to make these kinds of decisions in reality. In addition to conducting the elite survey with non-military space

experts, it would also be beneficial to have more senior military space officials complete the survey to see if there are differences in perspectives at a higher level of authority.

As with any experimental research method, a certain amount of artificiality is to be expected. In the case of both surveys, respondents are well removed from these actions happening in the real world, and notional attacks clearly do not carry the same gravitas as real-world attacks. Additionally, survey respondents had to make selections in a vacuum, free from interaction with other respondents, and without the benefit of a white cell to clarify information. Despite these challenges, the quality of justifications provided by respondents indicates that most people did take the surveys seriously and provided well-reasoned responses.

5.4 Conclusion

Neither the elite survey nor public opinion survey yielded data that were statistically significant enough to confirm my hypotheses, and as such I cannot reject the null hypotheses that entanglement status does not affect the decision to attack space systems. For the elite survey, entanglement appeared only to have deterred attacks against missile warning systems. No attacks were conducted against entangled missile warning systems, or the strategic/nuclear versions of the disentangled missile warning systems. Conventional missile warning systems were attacked as well as missile warning systems with unknown status, so clearly respondents believed there was some benefit to be gained from attacking those systems. For space security experts, an unacceptable risk of retaliation and escalation seemed only to exist only for NC3 missile warning systems, whereas ISR and SATCOM NC3 systems, as well as disentangled conventional missile warning systems did not enjoy such protection. These findings lend some support to

hypothesis 2, which asserts that disentangled versions of systems are viewed as less dangerous and therefore more likely to be attacked, though again, this only applied to missile warning.

Because elite survey respondents had awareness of the real-world U.S. NC3 architecture, it is possible that this knowledge could explain the differing values placed on missile warning systems compared to NC3 ISR and SATCOM systems. As discussed in Chapter 2, there are no commercial alternatives for missile warning systems and these systems are critical components of U.S. missile defense architecture. If these systems were destroyed, not only would strategic warning be greatly affected, but the U.S.' ability to defend against incoming threats would also be degraded. With ISR and SATCOM systems, there are commercial and other military options available for many of the functions these systems perform. In both the surveys and wargames this information was not provided to participants and NC3 systems were all treated equally. Elite survey respondents' real-world knowledge of these systems from a U.S. perspective could explain why only missile warning systems were treated uniquely.

For the public survey, entanglement yielded higher mean responses than other treatments, however the differences between treatments were not statistically significant. For the public surveys, alternative explanations were most potent. The most important factor influencing public responses was whether the attack was kinetic or non-kinetic, which was statistically significant. Additionally, proportional response was the primary justification given by public survey respondents and on average, mean scores corresponded to the type of attack conducted originally. For example, respondents who faced a cyber attack were most likely to recommend a cyber attack in response,

regardless of entanglement treatment. Attacks against disentangled conventional systems were viewed as less severe than entangled or disentangled strategic systems which provides support to hypothesis 2, though differences were more attributed to the type of attack than system attacked.

The lack of statistical significance across entanglement treatments for the surveys warrants further examination and bounds need to be set on what claims can be with respect to entanglement based on these findings. There are certainly differences in how survey respondents as a whole viewed disentangled nuclear and conventional systems, which is expected under the logic of my theory. Ultimately, however, these systems were not attacked more often than entangled systems. With that in mind, I cannot claim that entanglement affected decisions on whether or not to attack space systems (broadly) for survey respondents. With a relatively small sample size for the elite surveys, differences between treatments would've needed to be much more significant to make definitive claims about the effects of entanglement.

There are several possible justifications underpinning the null findings for the surveys, some of which have been discussed previously. For the elite survey, it is possible that real-world knowledge of U.S. systems, doctrine, and policies was too strong of an influence to overcome. Another possible explanation is that elite respondents simply did not view attacks against space systems (particularly ISR and SATCOM) as being particularly dangerous or egregious. The most probable explanation for the results can be found in the qualitative feedback provided by respondents. According to some respondents, entanglement was a significant factor and deterred attacks, but for others it was not as important as the objectives they sought to achieve through attacks. This

harkens back to a fundamental truth about deterrence. Whether or not a party is deterred is ultimately a choice. The deterrer could pursue strategies that logically should enhance deterrence and those strategies could still fail in some contexts and under some circumstances. Humans can respond to the same inputs in vastly different ways because each person brings a unique set of beliefs and goals and backgrounds to decision making, and that is exactly what played out with the surveys and that is an important consideration for all theories of decision making.

For other findings, elite survey respondents favored non-kinetic attack options, as was the case with the wargames, and cyber attacks again took precedence within this category. For the public survey, respondents viewed cyber attacks as being less severe and many cited the relative safety of cyber attacks in their justifications. These findings are consistent across experimental methods and could indicate possible future trends in space and terrestrial warfare. If cyber attacks are considered to be both safe and useful by the majority of respondents, it is reasonable to expect these sentiments are shared by other states within the international community. Additionally, the elite surveys demonstrated that respondents viewed their own attacks against adversary systems as being less severe than commensurate attacks against their systems. Whether prospect theory explains this tendency or if it is some other factor, this could be an important consideration for decision makers attempting to predict consequences for their attacks in the future.

CHAPTER 6. CONCLUSION

6.1 Overall Findings

This dissertation has investigated whether and how NC3 space system entanglement deters attacks against these systems. Using novel experimental wargames and surveys, I present the first empirical research that treats entanglement as an independent variable. As such, this research contributes much-needed empirical data to an under-represented area of scholarship. My theory of deterrence through entanglement asserts that potential adversaries expect severe retaliation for attacks against entangled NC3 space systems due to the impact these attacks would have on strategic capabilities of the targeted state. As such, challengers should be deterred from attacking these systems in any case short of full-scale war. Additionally, if these systems are disentangled, potential adversaries can attack disentangled versions of the systems without incurring as severe a response and are therefore more likely to conduct attacks.

Based on the broad recognition of the criticality of NC3 systems and the expectation of severe retaliation for attacks against these systems, I expected entangled NC3 systems to deter attacks more than disentangled conventional systems. My data have revealed that entanglement does affect adversary decisions on whether or not to attack space systems, but in different ways than I initially imagined. The space security wargames conducted with Georgia Tech students provide strong support to my theory, with entangled teams a third as likely to conduct attacks against NC3 space systems as disentangled teams. Additionally, when entangled teams did conduct attacks, they were less severe on average than disentangled or unknown status teams. Qualitative data from the wargames reinforce these findings, with entangled participants citing uncontrolled

escalation as the primary factor affecting their decisions to attack. Disentangled participants also provided confirmatory feedback in their justifications to attack conventional systems, with one participant expounding on the underlying logic of my theory quite succinctly, "of course it is safer to attack a conventional missile warning satellite than a nuclear one."[357]

Experimental surveys conducted with military space security elites do not provide such strong support to my theory. I found no statistical significance between entanglement treatment and decisions to attack NC3 space systems. There are a number of possible explanations for this, ranging from a greater propensity for hawkish actions by military members to the simplest explanation that many of these respondents simply did not consider the risks associated with attacking entangled systems to outweigh the perceived military advantage of the attacks. While my theory did not appear to gain traction broadly among this group, entanglement did deter attacks against missile warning systems. No attacks were conducted against entangled missile warning or disentangled strategic missile warning. In this case, entanglement ensured that even conventional attacks would affect nuclear capabilities of the targeted state, and unlike ISR and SATCOM systems, this created a red line that elite respondents were unwilling to cross. Feedback from entangled participants again cited escalation as being the primary concern affecting the decision to attack, and these respondents were three times more likely to avoid attacks out of fear of escalation as their disentangled and unknown status counterparts.

[357] Space Security Fall 2020, Participant 1

Finally, the public survey did not yield statistically significant evidence of the effect of entanglement treatment on responses The primary factors influencing responses were proportionality and the type of attack conducted initially. As expected, entangled respondents did recommend the most severe retaliation, but the variance within each of the treatments diluted the significance of the findings. Disentangled respondents also recommended much less severe retaliation for conventional system attacks than for strategic system attacks, as my theory predicts, but again variance made statistical significance impossible. Overall, the data from the public surveys suggest that the American public views non-kinetic attacks as being less severe than kinetic attacks, regardless of how/what systems are affected, and that most people support an in-kind retaliation to attacks.

In both the wargames and surveys, disentangled nuclear systems were least likely to be attacked of all, and there was broad recognition of the criticality of these systems. My theory asserts that potential adversaries expect the most severe consequences for attacks against a state's vital capabilities, so it is logical that if given a choice, participants would attack against systems explicitly used for nuclear missions. With entangled systems, an adversary could more credibly claim to have non-nuclear objectives; that is not the case with disentangled nuclear systems. That said, disentangled nuclear systems were still attacked in both wargames and surveys, despite the fact that these scenarios featured conventional objectives.

6.2 Revisiting Entanglement and Deterrence

There is a consensus among space security scholars that space systems are likely to be attacked in future conflicts, and previous wargames also suggest this to be the case.

Some scholars have claimed that NC3 space systems are particularly attractive targets in future conflicts due to the vital missions these systems support.[358] However, some of these scholars fear that the entangled nature of these systems could lead states to inadvertently escalate what would otherwise be regional or conventional conflicts due to attacks inherently affecting nuclear capabilities. As a result, the DoD has begun the process of disentangling NC3 space systems, and millions of dollars have already been spent to this end, despite warnings from the Government Accountability Office that the effects of disentanglement had not been studied and could incur additional risks.[359] The lack of empirical data to support real world policy decisions related to NC3 space system entanglement was the impetus for this research. Before new disentangled space systems are fielded, it is imperative to consider second and third order effects, namely the increased likelihood of attacks on disentangled conventional systems.

Most of the existing literature on entanglement has focused on inadvertent escalation in a terrestrial context, and comparatively little has been written about space system entanglement.[360] The general concept of inadvertent escalation as a result of entanglement is logically sound. Entangled systems are likely to be attacked in regional or lower-level conflicts, these attacks could affect the targeted state's nuclear capabilities, nuclear capabilities are vital interests to states and demand retaliation, and as a result the conflict will escalate. I do not dispute that this scenario is possible, however, other

[358] Harrison, T. et al. (2017); Cheng, D. (2012); Acton, J. (2018); Arbatov, A., Dvorkin, V. and Topychkanov, P. (2017); Zhang, B. (2011); Zhao, T. and Bin, L. (2017); Air Force Space Command (2016); Defense Intelligence Agency (2019); National Air and Space Intelligence Center (2018)
[359] Government Accountability Office (2014), 11.
[360] There are a number of works that discuss entanglement and how it contributes to escalation in the terrestrial domain, including: Posen, B. (1991); Pollack, J. (2009); Cunningham, F. and Fravel, M. (2015); Rovner, J. (2017). There are also some works that discuss space system entanglement and escalation: Zhao, T. and Bin, L. (2017); Arbatov, A., Dvorkin, V., and Topychkanov, P. (2017); Tannenwald, N. and Acton, J. (2018); Acton, J. (2018, 2020).

scholars have recently called into question the likelihood of inadvertent escalation as a result of entanglement. One of the leading voices in inadvertent escalation literature, Barry Posen, acknowledged in 1991 that "we have no examples of such escalation," and in the two decades since there is still "no evidence of dual-capable systems ever producing nuclear escalation in the empirical record."[361] Perhaps entangled space systems possess unique characteristics that make inadvertent escalation more likely if they are attacked, perhaps not. Kroenig and Massa have argued that the hypothetical escalation cases generated by entanglement theorists are "logically inconsistent, lack strategic empathy, and do not account for operational obstacles to nuclear preemption."[362] These cases are hardly sufficient to justify millions of dollars of investment and sweeping changes to space system design and infrastructure.

I do not directly test inadvertent escalation through my research, aside from the initial input for wargaming Scenario 2. As a reminder, this input was designed to assess whether participants would assume that a satellite malfunction during a crisis was an attack (which is a concern presented by Acton and others). Despite the input telling participants that a cyber attack was suspected, and that the system affected was a critical missile warning satellite, only 4 of the 37 teams that received this input chose to conduct any type of counter attack in their opening moves. This lends more support to the argument that inadvertent escalation has been overstated by entanglement theorists. However, the most important takeaway from all of this is that existing literature and policy decisions have been focused on inadvertent escalation, while ignoring the possible benefits of entanglement, namely deterrence. While very little has been written

[361] Posen, B. (1991), 4; Kroeinig, M. and Massa, M. (2021), 1.
[362] Kroenig, M. and Massa, M. (2021), 3.

previously about deterrence as it relates to space system entanglement, some scholars have suggested this as a possibility in the past.

Both China and Russia have entangled NC3 space systems as well as nuclear and conventional military forces. James Acton says that in Russia's case, this decision is more a function of budgets and administrative issues rather than a deliberate deterrence measure, however, he acknowledges that there could be deterrence value with entanglement.[363] Cunningham and Fravel say that comingling (entanglement) indicates "China's efforts to intentionally increase the risk of nuclear escalation in the event of a U.S. conventional strike on its missile bases."[364] According to Kroenig and Massa "countries may intentionally pursue deterrence through entanglement" because "leaders might conclude that attacking dual-use capabilities is too risky."[365] Going back to Mearsheimer, deterrence "means persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks."[366] Inadvertent escalation theorists believe that the vital importance of NC3 systems compels states to retaliate in response to attacks in a severe manner (hence inadvertent escalation), whether to preempt further attacks or to hedge against a nuclear attack crippling second-strike capabilities. Using this same logic, potential adversaries can assume that attacks against NC3 systems will be met with severe, and possibly nuclear, retaliation. If a state has limited objectives, short of full-scale war, they should be persuaded not to conduct attacks against entangled NC3 space systems, because the costs cannot be justified. This is the essence of my theory.

---

[363] Acton, J. (2017), 2; Acton, J. (2018)
[364] Cunningham, F. and Fravel, M. (2015), 45.
[365] Kroenig, M., and Massa, M. (2021), 11.
[366] Mearsheimer, J. (1985), 14.

6.3 Relevance to Other Areas

While my research has filled in some gaps in our understanding of NC3 space system entanglement, the findings raise additional questions that should be explored. One of the most significant findings that has relevance to other areas of research is the willingness of respondents across all experiments to employ cyber weapons. Not only were these weapons viewed as safe options, participants did not view cyber attacks as warranting the same level of response compared to other types of attacks, both as the attacker and victim. Wargaming participants also used cyber weapons against space systems as part of their diplomacy strategy, unrelated to military operations, and indicated that these attacks existed in a "grey area" between soft and hard power.

These findings add support to similar recent research conducted by Jacquelyn Schneider, Benjamin Schechter, and Rachael Shaffer. The researchers conducted crisis wargames to assess cyber operations and found that these operations did not have a significant impact on crisis escalation, and were used to "shape narratives as a complement to diplomacy prior to war and then as a support to military operations after was has escalated."[367] These findings also build on previous research conducted by Sarah Kreps and Jacquelyn Schneider, in which the authors gauged public support for retaliation based on not only the means of attack (cyber, conventional, or nuclear), but also the effects of the attacks (treasure, blood, and nuclear). They found that "Americans are less likely to support retaliation with force when the scenario involves a cyberattack even when they perceive the magnitude of attacks across domains to be comparable" and

[367] Schneider, J., Schechter, B. and Shaffer, R. (2022), 1.

that "for the American public, cyberattacks are qualitatively different" than other types of attacks.[368]

Taken together with my own research, these findings suggest a very real disparity in perceptions of cyber attacks compared to other types of attacks and could indicate that new approaches to escalation and deterrence in the cyber domain are needed. More importantly for my line of investigation, if state leaders share these beliefs, cyber attacks in space could become much more likely. With the already difficult task of defending against and attributing cyber attacks combined with the difficulty in attributing space system anomalies and attacks, these beliefs could be particularly dangerous and create significant risks of misperception and inadvertent escalation in space.

Another area of research that deserves renewed attention is the role of human nature and psychology in decision making. While constructivists have championed individual-level analyses and promoted leader-centric theories in international relations, much of IR scholarship continues to emphasize states as black box rational actors and ignores the possible effects of human cognition. The elite survey demonstrated significant differences in perceptions of attack severity based on whether the respondent was the attacker or victim, which is probably best explained with behavioral economics and prospect theory. These differences in perceptions could play an important role when leaders attempt to identify likely costs associated with their actions. Based on the findings from my surveys, leaders are likely to underestimate the severity with which their actions will be perceived, and retaliation could be more severe than expected.

[368] Kreps, S. and Schneider, J. (2019), 1, 8.

6.4 Contributions to Scholarship

My research contributes to space security and entanglement scholarship in a number of ways. Most importantly, this is the first-ever empirical analysis of space system entanglement. While scholars have conducted space security wargames, elite and public surveys, and other types of space security analyses in the past, none have used entanglement as a variable. This is particularly concerning considering the real-world decisions being made about entangled space systems without data to support these decisions. The Government Accountability Office recommended studies to test the effects of disentanglement over 7 years ago, and no such studies have been conducted until now; at least not in open-source reporting. More broadly, my research further demonstrates the possibility and utility in experimental approaches to space security studies. Assessing these issues in the real-world is impossible, so researchers must rely on novel approaches to test space security concepts.

Importantly, through my research I have challenged widely held beliefs that disentanglement contributes to deterrence and demonstrated that not only are disentangled systems more likely to be attacked in future conflicts, but they will also likely face more severe attacks than entangled systems due to the perceived lower risk of escalation. This finding alone should give pause to leaders advocating for increased disentanglement in the U.S.' NC3 architecture. I also challenge the notion that disentangled nuclear systems will be viewed as "clearly off limits," as these systems were attacked in both the wargames and elite surveys. If this assumption is being used to inform policies and strategies within the U.S. government, my research shows that this could be a dangerous misperception. My research also builds upon the recent work of

Kroenig and Massa and challenges claims about the likelihood of inadvertent escalation in response to attacks against NC3 systems. Although I did not test escalation directly as a DV, I did assess inadvertent escalation related to perceived attacks with Scenario 2 of the wargames and found that the risk of inadvertent escalation has been overstated. Overall, my research provides new data with which to assess entanglement and perceptions about space conflict, both from elite populations and the public. These data can be used to inform better policies and strategies for space moving forward.

6.5 Policy Implications

Based on my findings, I have the following four recommendations for policy makers. Some of these recommendations are materiel solutions while others pull on soft power and diplomatic levers:

Evaluate Objectives of Entanglement

Contrary to the current DoD motto of "embrace disaggregation," I recommend that the DoD take a more critical approach with respect to entanglement. While entanglement does not provide absolute deterrence, neither does disentanglement, as even disentangled nuclear systems were attacked in both wargames and elite surveys. Even though disentangled nuclear systems were least likely of all to be attacked, the attacks that did occur are particularly worrisome because none of the participants who attacked nuclear versions of disentangled systems intended to start a nuclear exchange. In the real world, such attacks might warrant even more severe retaliation than attacks against entangled systems due to the unambiguous message that such an attack would convey. In these cases, entanglement could provide leaders with more decision space and flexibility than disentanglement because the systems are both strategic and tactical. Entanglement

allows both the aggressor and victim plausible avenues to interpret attacks as constituting something less egregious, if they so choose. This would be less likely if disentangled nuclear systems were attacked. More importantly though, entanglement keeps *expected* costs to attackers high, even if victims choose not to respond as severely. Attacks against disentangled conventional systems were widely viewed across all wargames and surveys as being less severe, which is ultimately a dangerous prospect for these systems.

Though I did not delve deeply into the other types of space system entanglement, my recommendation to embrace entanglement applies broadly. The core logic of my theory is that entangled systems incur higher costs for attacks, and as others have argued, this could be true of entanglement between commercial and military systems, foreign partner systems, and many other configurations. If a potential adversary has to disable commercial communications, or the ISR capabilities of other states, they could be even more likely to conclude the costs outweigh the benefits. Of course there are security considerations with shared systems, but those have been effectively managed over the last 20 years of commercial SATCOM use and increased reliance on commercial ISR.

There is a more fundamental issue with the logic of disentanglement as well. Any competent adversary would need to assume that disentangled strategic systems could also be used to perform the functions that disentangled conventional systems performed. For example, a disentangled strategic ISR satellite that had the stated purpose of treaty verification and I&W for missile launches could also clearly be used to support tactical operations. Would a potential adversary believe that attacking only the disentangled conventional system was sufficient to conceal their operations? Unlikely. The same holds true for SATCOM and missile warning. To do any meaningful damage and truly gain

asymmetric advantage, both versions of systems would need to be attacked, and if that is the case, disentanglement really does not gain anything. This issue is addressed further in my next recommendation.

Establish Norms, Laws, and Thresholds -

Many participants in the wargames cited difficulty in understanding expectations of escalation, the use of force, and what constituted an armed attack in space. There have been some efforts to apply international law to space conflict, but as of now no formal guidelines have been established.[369]A number of participants indicated that they were unsure what type of response would be expected based on their actions, which made it more difficult to manage risks. These difficulties are not exclusive to students; indeed, these topics are a source of debate throughout the global space community. The U.S. maintains a flexible response posture in space, as in other domains, which allows for a response in a time, domain, and manner of their choosing, but there are no escalation thresholds or clearly defined limits. According to a report from the RAND Corporation "U.S. analysts cannot predict with certainty how their own government would be likely to react to many sorts of potential attacks, such as the deliberate destruction of U.S. satellites."[370] Recently, the head of Russia's space agency, Dmitry Rogozin, said that "offlining the satellites of any country is actually a casus belli, a cause for war," but it's unclear what types of attacks and what types of satellites this applies to.[371]

The ambiguity in this area could deter attacks, as potential adversaries might not want to test their fate with uncertain consequences, but the ambiguity could also lead

[369] Nasu, H. (2022).
[370] Morgan, F. et al. (2008), 14.
[371] Moscow bureau (2022).

states to underestimate the effect their attacks would have on others. Some wargaming participants claimed that uncertainty constrained their actions, while others felt the uncertainty gave more flexibility to attack first and then negotiate consequences. While it might not be feasible or advisable to establish formal red lines in space, it would be beneficial to at least identify which types of attacks and against which systems are particularly egregious. In order to do this, states first need to agree on what constitutes an attack, and more broadly, what responsible operations in space look like. As it stands now, space is the "wild west" with a massive proliferation in objects and operators in space, and almost no governance.[372] The first step to instilling order in the domain is to create norms, laws, and thresholds that the international community can abide by.

Finally, in order to support laws, norms, and thresholds, states should clearly communicate the purpose and capabilities of their systems. Gone are the days when states could hide capabilities in plain sight in space. Improvements in remote sensing technologies, both by governments and commercially, have enabled high-resolution satellite inspections and continuous tracking of previously unknown objects. Both Russia and China have concealed satellites and capabilities that the U.S. identified, which leads to increased tension and mistrust in space.[373] Space operators need to be aware of what types of systems are operating near their spacecraft, and more importantly for my research, deterrence through entanglement cannot work if states conceal the functions and status of their spacecraft.

[372] Everstine, B. (2021).
[373] Gruss, M. (2015).

Improve Attribution -

Attribution is critical in the space domain, not only for deterrence, but for routine operations. The ability to attribute attacks is an essential element for deterrence, otherwise there can be no credible threat of retaliation. Additionally, attribution can prevent inadvertent escalation by enabling operators to identify the source of malfunctions and anomalies, whether they are hostile or not. In both the surveys and wargames, participants regularly cited cyber attacks as being a safe option because of the difficulty in attributing these kinds of attacks. Some of these participants could have been deterred from these attacks if attribution were more certain. There are many ways to improve attribution, including investments in space domain awareness, cyber threat detection capabilities, and cooperation and data sharing with other space operators, but ultimately any deterrence strategy in space necessarily includes improved attribution.

6.6 Future Research and Closing Thoughts

In order to observe the effects of entanglement directly, I had to limit the number and types of variables I tested. While this is common in experimental settings, it does not always capture the full scope of causal factors in decision making. I was also constrained by the need to avoid classification issues, which is challenging in the heavily-compartmented space domain. These issues do not detract from the validity of my research, rather they provide room to expand this research and incorporate new variables and systems. To begin with, it would be useful to conduct entanglement-focused wargames in a classified setting using real states and real systems (both weapons and targets). This would allow for much greater fidelity with respect to system impacts and would provide a clearer picture of effects to the overall NC3 architecture. Orbital

modeling software could be used to propagate debris fields for kinetic attacks and to determine what regions and missions were affected for other non-kinetic attacks. For example, a blinding attack against an NC3 LEO ISR satellite has some notional impact on wargaming and survey participants in my research, however, if real systems and modeling could be used, participants could identify which imagery collection targets would be lost over a given period and determine real-world degradations in ability to provide indications and warnings. The same goes for the other systems I investigate. Ultimately, this is the type of data that leaders need to make informed decisions about retaliation.

Another benefit of using real world systems and threats is that probabilities of success and attribution could be more accurately assessed. Some systems have protections against some types of threats, but it would be too challenging to incorporate these satellite-level defenses into my current research. It would also be possible for "red team" participants to make more informed decisions about what systems to attack and how to attack them if real-world systems were used. In a real setting, a potential adversary would have intelligence about satellite defenses, resilience, and orbits that would all be required to accurately target space systems.

Military operations are frequently planned around when space effects are most available, and a savvy adversary would know when attacks against space systems could generate the most bang for the buck. For example, despite a massive proliferation in remote sensing platforms, all areas on earth cannot be covered all the time. A well-timed attack against imagery satellites that are due to pass over a desired location could buy a big enough window to conduct operations without being detected. The number of

satellites that would need to be attacked is entirely dependent on the location, time of day, weather conditions, scale of operations, and a host of other factors that simply cannot be incorporated into notional experiments.

Again for simplicity, I bundled all NC3 space systems together for entanglement status. It would be useful, however, to investigate varying levels of entanglement by system type. My research revealed a hesitancy to attack entangled and disentangled strategic missile warning systems, but no such hesitancy existed for ISR systems. It would be useful to test an entangled missile warning constellation with a disentangled ISR constellation, or a partially entangled SATCOM architecture. Perhaps some systems are more affected by entanglement, or perhaps there is some equilibrium point with entanglement and disentanglement that deters attacks. Even more valuable would be incorporating other variables that could influence deterrence in the space domain, like resilience. How does a resilient entangled architecture compare to a resilient disentangled architecture? Does resilience plus entanglement lead to greater deterrence, and does this provide decision makers greater flexibility in their responses? Previous research has demonstrated the value of resilience, but entanglement has not been included.

In addition to changing the IVs for this research, it would be beneficial to look at different DVs as well. Much of the existing literature about entanglement focuses on inadvertent escalation, so it would be useful to use escalation as a DV. There are two ways in which escalation can be measured as it relates to the space security scenarios. The first is to use Kahn's "three ways to escalate a limited conflict" model to determine if escalation has occurred. Under this model, escalation has occurred if there is an increase in intensity, widened area, or compounded escalation, which could involve violating

sanctuary or involving other participants.[374] Another way to measure escalation is to place each action taken by participants on a rung on Kahn's escalation ladder. Any action that moves to a higher rung on the ladder could be viewed as escalation. Escalation should be viewed both from the standpoint of actions taken by the targeted state relative to the actions that state was taking previously, as well as actions relative to the attack conducted. In this way, it would be possible to observe how entanglement affects escalation, rather than deterrence.

Introducing new IVs and DVs would increase our understanding of escalation and deterrence in the space domain, but a key factor for improving the generalizability of this research would be to conduct experiments outside of the U.S. The impressive diversity at Georgia Tech afforded me the opportunity to include many foreign students in my wargames, but these students were not singled out or grouped based on nationality, so I did not conduct any analysis into trends based on country of citizenship. In Chapter 2 I discussed how both China and Russia have incorporated ASATs into their military strategies, and the differing views within both countries regarding expected costs of attacks. Both states have also entangled their NC3 systems to some extent, whether for deterrence or for economic and administrative reasons. The U.S., China, and Russia all see each other as threats in space, so it would be interesting to conduct my wargames and surveys within both countries to see what differences exist in perceptions about risk and reward. It would also be useful to conduct the research with U.S. allies who depend on and contribute to the NC3 systems I investigate. States without robust organic space capabilities might be more sensitive to losses and more risk averse than U.S. participants

[374] Kahn, H. (1965). On Escalation: Metaphors and Scenarios. New York, NY: Frederick A. Praeger, Publishers, 4.

who are accustomed to immense space infrastructure. Finally, as mentioned in Chapter 5, I would like to conduct my surveys with more senior leaders, both within and the U.S. and abroad. It was useful to observe respondents from the population likely to be involved in campaign planning, but it would also be useful to observe the leaders that would ultimately decide what options to employ.

A broader area of investigation that arose from my research was the impact of real-world events on experimental settings. As I discussed in Chapter 4, the Russian invasion of Ukraine the day of one of my wargaming sessions had a significant impact on the actions of participants. Among the 84 teams who participated in the wargames, there were 37 non-space military attacks conducted. Over half of these attacks (n = 19) were conducted by the 12 teams from that one wargaming session. Fifty-one percent of all non-space military attacks were conducted by just 14% of teams. During this wargaming session, only 1 of 12 teams did not deploy military forces, and fully half of the teams (6 of 12) conducted attacks against ground forces. Conventional attacks against ground forces were selected by only 1 of the other 72 teams (1.39%) that participated in the wargaming scenarios. These findings suggest an important consideration for future experimental research. Participants could be biased not only by the experimental design, but also by events transpiring in the world external to the experiments. This is not some new revelation, as researchers have known for decades that "contextual factors that are beyond the control of the experimenter may have equally profound impacts on actions," however, it is interesting to see how profound these impacts can be, as in the case of my research.[375] It is also difficult to measure this because researchers would have to wait for

[375] List, J. and Levitt, S. (2005), 5.

events to transpire around the world related to the area of study and then complete their experiments, so my research just happened to provide this coincidental opportunity to observe the power of bias based on external context.

The research presented in this dissertation adds new empirical data to refine our understanding not only of entanglement, but also perceptions about the use of space weapons. More broadly, this research increases our awareness of factors that affect deterrence and stability in space. My theory of deterrence through entanglement could be useful in shaping future policies in space as well as inform future space system acquisitions strategies. My research has demonstrated that absolute deterrence is unlikely, but it has also shown there are possible avenues to limit attacks against some types of systems under some configurations. The future research presented in this section could further expand our understanding of the dynamics of space security and hopefully lead to a more secure future in the space domain. Conflict in space might be inevitable, it might not be, but the best way to ensure we do not lose access to critical capabilities enabled by this vital domain is to not limit our focus on technology alone, but also consider the human decision makers that will determine whether conflict occurs in space moving forward. Fortunately, and unfortunately, humans are the greatest threat to space security, but humans can also be deterred.

APPENDIX A. WARGAMING SCENARIOS

Wargaming Background - All Scenarios and Treatments

The State of the Space Environment

Purple has been the global leader in terms of space capability, development, and technology for many decades. Purple draws on their robust military, civilian, and commercial space sectors to enable many aspects of their nation's functions. Purple is heavily dependent on space for nearly all aspects of their military operations, so they devote significant resources toward protecting and defending their military space capabilities. Yellow pioneered many space capabilities in the early ages of space operations but declined as a peer competitor to Purple as internal diplomatic and economic issues drew attention and resources away from their space program. In spite of the decline, Yellow possesses a highly capable national security space infrastructure, particularly with their Intelligence, Surveillance, and Reconnaissance (ISR) and Missile Warning systems. Green is an emerging global competitor with a motivated and educated population, as well as significant resources to devote to advancing their space capabilities. Green's military space capabilities are not nearly as robust as Purple or Yellow, but they are quickly advancing on the space weapons front. Recently, Yellow has re-focused on the space domain to better compete with purple and to limit the advancement of Green.

The State of Space Situational Awareness

Purple, Green, and Yellow participate in an international agreement/organization to coordinate use of the geosynchronous orbit (GEO) for both satellite positioning and radio frequency (RF) spectrum allocation. Failure to comply with either parameter could negatively affect the operations of other spacecraft in the vicinity. Purple, Green, and Yellow also share satellite positioning data with an international agency that maintains a space object database that can be accessed by anyone. The missions performed by spacecraft should be published as well, but there have been many cases of deception from each of the major space powers. Purple also publishes a space catalog based on data collected from their SSA sensors and they also issue warnings to operators when a collision is forecasted/imminent. Green and Yellow also maintain fairly robust and sophisticated space object surveillance and identification (SOSI) networks, though they do not publish their data publicly.

The State of the Terrestrial Environment

Purple has a sophisticated conventional military and employs the most advanced and capable Air and Naval forces in the world. Purple's land forces are also highly capable and equipped with the best technology in the world. Green has a huge population that enables land force capability sheerly through size. They have the largest land force in the world and are rapidly advancing their air and naval capabilities. Yellow has aging land, air, and naval forces and equipment and is not advancing their capabilities at the same rate as Purple and Green. Yellow is instead more focused on competing in the space and cyber domains and generating asymmetric effects through those capabilities.

The State of Space Law/Policy

Non-nuclear space weapons are not prohibited by international law, and there are no universally accepted norms for space operations. The use of kinetic space weapons has not occurred previously, but all three states have developed and tested space weapons that they believe are permitted under international law. All three states in these scenarios have indicated their primary objective is to deter space conflict and prevent the use of weapons in space, though all maintain the ability and intent to deny or degrade other states' space capabilities in order to preserve the use of their own systems, if required. None of the states trust the other states to not use space weapons and each of the three states in these scenarios have accused the others of irresponsible and escalatory actions in the past/present.

The State of Counterspace Weapon Testing and Development

None of the major space powers in these scenarios have intentionally destroyed space systems of another state, though all have demonstrated the capability to do so through tests on their own systems. All three actors possess a range of space weapons from kinetic to non-kinetic, reversible/temporary to permanent. The verbiage in the table below is taken directly from a space crisis exercise performed by the Center for Strategic and International Studies, only the country names and minor details have been altered. The CSIS space weapons background table is being used in these scenarios because it presents a fictional yet realistic view into the capabilities and employment of space weapons by major space powers.

Wargaming Response Options - All Scenarios, Entangled and Unknown Treatments

Diplomatic / Economic / Informational	
Public	• **Send public demarche** • **Propose bilateral discussions** • **Impose economic sanctions** • **Request military support from allies**
Private	• **Send private demarche** • **Propose secret bilateral discussions** • **Leak information or disinformation to media**
Non-Space	
Non-Kinetic	• **Raise/lower the alert status of forces in the region** • **Deploy/withdraw aircraft in the region** ○ Specify manned/unmanned, armed/unarmed • **Deploy/withdraw maritime forces in the region** • **Deploy/withdraw ground forces in the region**

Kinetic	• **Declare a no-fly zone and give shoot-down authority**
	• **Attack maritime forces**
	  ○ Success 90%, Attribution 100%
	• **Attack ground forces**
	  ○ Success 90%, Attribution 100%
	• **Conduct targeted special operations**
	  ○ Success 80%, Attribution 80%

Space	

Non-Kinetic	• **Jam commercial/military SATCOM downlinks (localized)**
	  ○ Success 90%, Attribution 90%
	  ○ Specify system(s) (Success
	• **Jam protected SATCOM downlinks (localized)**
	  ○ Success 80%, Attribution 90%
	• **Jam commercial/military SATCOM uplinks (wide-area)**
	  ○ Affects users across region (Success 90%, Attribution 80%)
	• **Jam protected SATCOM uplinks**
	  ○ Affects users across region (Success 70%, Attribution 90%)
	• **Jam civilian/military PNT signal (local)**
	  ○ Specify civil/military (Success 90%, Attribution 90%)
	• **Jam civilian/military PNT signal (wide-area)**
	  ○ Specify civil/military (Success 70%, Attribution 90%)
	• **Cyber attack satellites**
	  ○ Specify ISR, missile warning, PNT, and/or commercial/military/protected SATCOM
	  ○ Success 70%, Attribution 60%
	• **Cyber attack C2 nodes**
	  ○ Specify ISR, missile warning, PNT, and/or commercial/military/protected SATCOM
	  ○ Success 60%, Attribution 50%
	• **Cyber attack missile warning radar(s)**
	  ○ Specify local/global
	  ○ Success 70%, Attribution 50%
	• **Dazzle/Blind ISR satellites**
	  ○ Success 70% dazzle / 30% blind, Attribution 80%
	• **Dazzle/Blind missile warning satellites**
	  ○ Success 70% dazzle / 30% blind, Attribution 80%

Kinetic	• **Move co-orbital ASATs near GEO satellites**
	  ○ Specify missile warning, commercial/military/protected SATCOM (Attribution 80%)
	• **Use co-orbital ASATs against GEO satellites**
	  ○ Specify missile warning, commercial/military/protected SATCOM (Success 90%, Attribution 90%)
	  ○ Produces debris
	• **Use direct-ascent ASAT against LEO ISR and/or MEO PNT satellites**
	  ○ Success LEO ISR 90% / MEO PNT 70%, Attribution 90%
	  ○ Produces debris
	• **Attack C2/SSA/Radar facilities in region/homeland**
	  ○ Specify target/location
	  ○ Success region 90% / homeland 20%, Attribution 100%

Wargaming Response Options - All Scenarios, Disentangled Treatment

Diplomatic / Economic / Informational	
Public	• **Send public demarche** • **Propose bilateral discussions** • **Impose economic sanctions** • **Request military support from allies**
Private	• **Send private demarche** • **Propose secret bilateral discussions** • **Leak information or disinformation to media**
Non-Space	
Non-Kinetic	• **Raise/lower the alert status of forces in the region** • **Deploy/withdraw aircraft in the region** ○ Specify manned/unmanned, armed/unarmed • **Deploy/withdraw maritime forces in the region** • **Deploy/withdraw ground forces in the region**

Kinetic	• **Declare a no-fly zone and give shoot-down authority**
	• **Attack maritime forces**
	  ○ Success 90%, Attribution 100%
	• **Attack ground forces**
	  ○ Success 90%, Attribution 100%
	• **Conduct targeted special operations**
	  ○ Success 80%, Attribution 80%

Space	

- **Jam commercial/military SATCOM downlinks (localized)**
  - Success 90%, Attribution 90%
  - Specify system(s) (Success
- **Jam protected SATCOM downlinks (localized)**
  - Specify strategic/nuclear or conventional/tactical satellites
  - Success 80%, Attribution 90%
- **Jam commercial/military SATCOM uplinks (wide-area)**
  - Affects users across region (Success 90%, Attribution 80%)
- **Jam protected SATCOM uplinks**
  - Specify strategic/nuclear or conventional/tactical satellites
  - Affects users across region (Success 70%, Attribution 90%)
- **Jam civilian/military PNT signal (local)**
  - Specify civil/military (Success 90%, Attribution 90%)
- **Jam civilian/military PNT signal (wide-area)**
  - Specify civil/military (Success 70%, Attribution 90%)
- **Cyber attack satellites**
  - Specify ISR, missile warning, PNT, and/or commercial/military/protected SATCOM
  - Specify strategic/nuclear or conventional/tactical satellites
  - Success 70%, Attribution 60%
- **Cyber attack C2 nodes**
  - Specify ISR, missile warning, PNT, and/or commercial/military/protected SATCOM
  - Specify strategic/nuclear or conventional/tactical nodes
  - Success 60%, Attribution 50%
- **Cyber attack missile warning radar(s)**
  - Specify local/global
  - Success 70%, Attribution 50%
- **Dazzle/Blind ISR satellites**
  - Specify strategic/nuclear or conventional/tactical satellites
  - Success 70% dazzle / 30% blind, Attribution 80%
- **Dazzle/Blind missile warning satellites**
  - Specify strategic/nuclear or conventional/tactical satellites
  - Success 70% dazzle / 30% blind, Attribution 80%

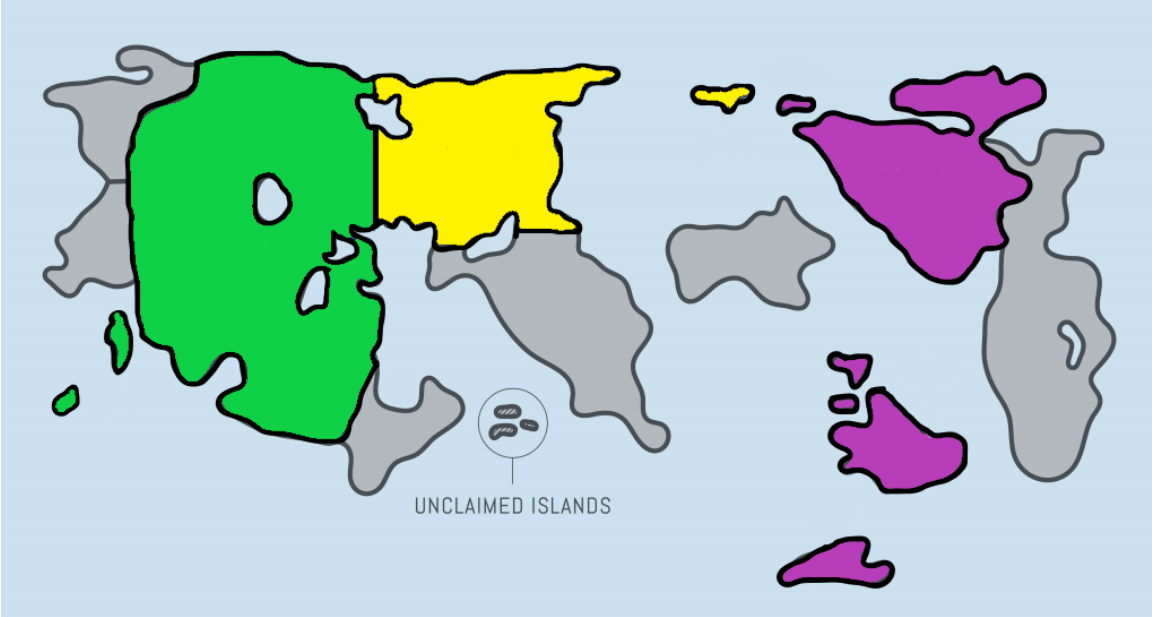
- **Move co-orbital ASATs near GEO satellites**
  - Specify missile warning, commercial/military/protected SATCOM (Attribution 80%)
- **Use co-orbital ASATs against GEO satellites**
  - Specify missile warning, commercial/military/protected SATCOM (Success 90%, Attribution 90%)
  - Specify strategic/nuclear or conventional/tactical satellites
  - Produces debris
- **Use direct-ascent ASAT against LEO ISR and/or MEO PNT satellites**
  - Success LEO ISR 90% / MEO PNT 70%, Attribution 90%
  - Specify strategic/nuclear or conventional/tactical satellites
  - Produces debris
- **Attack C2/SSA/Radar facilities in region/homeland**
  - Specify target/location
  - Specify strategic/nuclear or conventional/tactical systems
  - Success region 90% / homeland 20%, Attribution 100%

Wargaming Rules - All Scenarios and Treatments

- Teams will consist of 1-2 people, each team will be assigned a number for tracking and to avoid collecting personal information; all members of the team should contribute to decision making.
    - At least one team member should take notes on discussion high points and rationale for decisions
    - Teams will be mixed by degree/level, age, and gender to enhance diversity of thought/experience
- Teams will be paired, with one team representing one of the two states involved in the scenario, and the other team representing the other state
    - The White Cell will represent the third (or other) states if required during the scenario
    - Competition/adjudication will occur among pairs of teams, not between pairs
    - Teams and pairs will be physically separated to prevent unauthorized "intelligence" collection
- Teams may select up to 3 options per round for adjudication by the White Cell, and will write their decisions on the provided paper, along with very brief notes for why they chose those options.
    - Teams must select at least one option for each Move
- The White Cell will provide status updates or executive directives, as needed, throughout scenario execution
- Teams may not negotiate or discuss moves with other teams directly, all adjudication will be handled by the White Cell
    - Adjudication results will be announced to each pair to let teams know the results of their own and their paired team's decisions.
    - This is necessary to account for attribution and success variables, as well as to ensure decisions remain within the options provided.
- Teams may ask clarifying questions to the White Cell at any point during scenario execution.
- Participants should take the scenarios seriously and make decisions as if real people, weapons, and systems are involved, despite the fictional states and events.
- Oral consent is required from each participant.

Wargaming Scenario 1

Map - All Teams



Green Team Briefing - Entangled

You are a senior strategist in the Ministry of Defence in the Kingdom of Green. In recent years, Green has become more adamant about the need to secure additional territory to project military forces and counter Purple's influence and alliances in the region. Green leadership now intends to launch a campaign to take control of previously unclaimed islands (depicted above) and would deploy maritime, air, and ground forces for this operation. Purple has threatened military intervention if Green attempts to take control of the islands.

Purple's intelligence surveillance, and reconnaissance (ISR) and missile warning satellites provide coverage over the islands and would alert Purple leaders to any actions taken by Green to seize the islands. Additionally, Purple's satellite communications (SATCOM) systems allow forward-deployed military forces near the unclaimed islands to communicate securely with Purple leadership globally. Green also possesses ISR, SATCOM, and missile warning satellites to cover the region.

Green leadership believes that attacking Purple's ISR, missile warning, and SATCOM satellites could enable Green to take control of the islands without being immediately detected and without Purple being able to effectively respond militarily. However, Green does not want to start a full-scale war with Purple, as Purple has superior military capabilities.

The same ISR, missile warning, and SATCOM systems that could be used by Purple to detect and respond to Green's attempts to take control of the unclaimed islands are also

part of Purple's nuclear command, control, and communication (NC3) architecture, which provides strategic nuclear warning (i.e. advanced warning of a nuclear attack) and missile defense (i.e. the ability to defend against incoming nuclear missiles) for Purple. The same applies to Green's ISR, protected SATCOM, and missile warning systems.

Both Purple and Green's stated policies are that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation for attacks against NC3 systems. Both states consider unfettered access to and use of its space systems to be a vital national interest.

Green leadership has asked for your recommendation for how to proceed.

Green Team Briefing - Disentangled

You are a senior strategist in the Ministry of Defence in the Kingdom of Green. In recent years, Green has become more adamant about the need to secure additional territory to project military forces and counter Purple's influence and alliances in the region. Green leadership now intends to launch a campaign to take control of previously unclaimed islands (depicted above) and would deploy maritime, air, and ground forces for this operation. Purple has threatened military intervention if Green attempts to take control of the islands.

Purple's intelligence surveillance, and reconnaissance (ISR) and missile warning satellites provide coverage over the islands and would alert Purple leaders to any actions taken by Green to seize the islands. Additionally, Purple's satellite communications (SATCOM) systems allow forward-deployed military forces near the unclaimed islands to communicate securely with Purple leadership globally. Green also possesses ISR, SATCOM, and missile warning satellites to cover the region.

Green leadership believes that attacking Purple's ISR, missile warning, and SATCOM satellites could enable Green to take control of the islands without being immediately detected and without Purple being able to effectively respond militarily. However, Green does not want to start a full-scale war with Purple, as Purple has superior military capabilities.

Purple and Green have two versions of their ISR, SATCOM, and missile warning systems. One version is part of their nuclear command, control, and communication (NC3) architecture, and is used to support strategic/nuclear missions (like nuclear attack warning and missile defense). The other version of the systems supports tactical/conventional missions, such as Green's campaign to take control of the unclaimed islands and Purple's ability to monitor these actions. Although it is not its primary mission, NC3 systems may be capable of providing support for tactical/conventional missions, if needed.

Both Purple and Green's stated policies are that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including

nuclear retaliation for attacks against strategic/nuclear NC3 systems. Both states consider unfettered access to and use of its space systems to be a vital national interest.

Green leadership has asked for your recommendation for how to proceed.

Green Team Briefing - Unknown

You are a senior strategist in the Ministry of Defence in the Kingdom of Green. In recent years, Green has become more adamant about the need to secure additional territory to project military forces and counter Purple's influence and alliances in the region. Green leadership now intends to launch a campaign to take control of previously unclaimed islands (depicted above) and would deploy maritime, air, and ground forces for this operation. Purple has threatened military intervention if Green attempts to take control of the islands.

Purple's intelligence surveillance, and reconnaissance (ISR) and missile warning satellites provide coverage over the islands and would alert Purple leaders to any actions taken by Green to seize the islands. Additionally, Purple's satellite communications (SATCOM) systems allow forward-deployed military forces near the unclaimed islands to communicate securely with Purple leadership globally. Green also possesses ISR, SATCOM, and missile warning satellites to cover the region.

Green leadership believes that attacking Purple's ISR, missile warning, and SATCOM satellites could enable Green to take control of the islands without being immediately detected and without Purple being able to effectively respond militarily. However, Green does not want to start a full-scale war with Purple, as Purple has superior military capabilities.

Both Purple and Green's stated policies are that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation. Both states consider unfettered access to and use of its space systems to be a vital national interest.

Green leadership has asked for your recommendation for how to proceed.

Purple Team Briefing - Entangled

In recent years, Green has become increasingly committed to expanding their territory and regional influence and has made efforts to claim previously unclaimed islands in international waters (depicted above). Historically, Purple has demanded these efforts be stopped and have deployed maritime forces in the region.

Recent classified intelligence reporting shows that Green is massing maritime, air, and ground forces, which could be a sign they intend to launch a military campaign to take the islands. Purple's intelligence surveillance, and reconnaissance (ISR) and missile warning satellites provide coverage over the unclaimed islands and would alert Purple leaders to any actions taken by Green to seize the islands. Additionally, Purple's satellite

communications (SATCOM) systems allow forward-deployed military forces near the unclaimed islands to communicate securely with Purple leadership. Green also possesses their own space-based capabilities to provide ISR, SATCOM, and missile warning in the region.

The same ISR, missile warning, and SATCOM systems that could be used to detect and respond to Green's attempts to take control of the unclaimed islands are also part of Purple's nuclear command, control, and communication (NC3) architecture, which provides strategic nuclear warning (i.e. advanced warning of a nuclear attack) and missile defense (i.e. the ability to defend against incoming nuclear missiles) for Purple. The same applies to Green's ISR, protected SATCOM, and missile warning systems.

Both Purple and Green's stated policies are that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation for attacks against NC3 systems. Both states consider unfettered access to and use of its space systems to be a vital national interest.

Purple leadership does not want to start a full-scale war with Green, but cannot allow Green to take the islands as it would challenge Purple's position in the region and make allies in the region fear Purple's commitment.

Purple leadership has asked for recommendations for how to proceed.

Purple Team Briefing - Disentangled

In recent years, Green has become increasingly committed to expanding their territory and regional influence and has made efforts to claim previously unclaimed islands in international waters (depicted above). Historically, Purple has demanded these efforts be stopped and have deployed maritime forces in the region.

Recent classified intelligence reporting shows that Green is massing maritime, air, and ground forces, which could be a sign they intend to launch a military campaign to take the islands. Purple's intelligence surveillance, and reconnaissance (ISR) and missile warning satellites provide coverage over the unclaimed islands and would alert Purple leaders to any actions taken by Green to seize the islands. Additionally, Purple's satellite communications (SATCOM) systems allow forward-deployed military forces near the unclaimed islands to communicate securely with Purple leadership. Green also possesses their own space-based capabilities to provide ISR, SATCOM, and missile warning in the region.

Purple and Green have two versions of their ISR, SATCOM, and missile warning systems. One version is part of their nuclear command, control, and communication (NC3) architecture, and is used to support strategic/nuclear missions (like nuclear attack warning and missile defense). The other version of the systems supports tactical/conventional missions, such as Green's suspected campaign to take control of the unclaimed islands and Purple's ability to monitor these actions. Although it is not its

primary mission, NC3 systems may be capable of providing support for tactical/conventional missions, if needed.

Both Purple and Green's stated policies are that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation for attacks against strategic/nuclear NC3 systems. Both states consider unfettered access to and use of its space systems to be a vital national interest.

Purple leadership does not want to start a full-scale war with Green, but cannot allow Green to take the islands as it would challenge Purple's position in the region and make allies in the region fear Purple's commitment.

Purple leadership has asked for recommendations for how to proceed.

Purple Team Briefing - Unknown

In recent years, Green has become increasingly committed to expanding their territory and regional influence and has made efforts to claim previously unclaimed islands in international waters (depicted above). Historically, Purple has demanded these efforts be stopped and have deployed maritime forces in the region.

Recent classified intelligence reporting shows that Green is massing maritime, air, and ground forces, which could be a sign they intend to launch a military campaign to take the islands. Purple's intelligence surveillance, and reconnaissance (ISR) and missile warning satellites provide coverage over the unclaimed islands and would alert Purple leaders to any actions taken by Green to seize the islands. Additionally, Purple's satellite communications (SATCOM) systems allow forward-deployed military forces near the unclaimed islands to communicate securely with Purple leadership. Green also possesses their own space-based capabilities to provide ISR, SATCOM, and missile warning in the region.

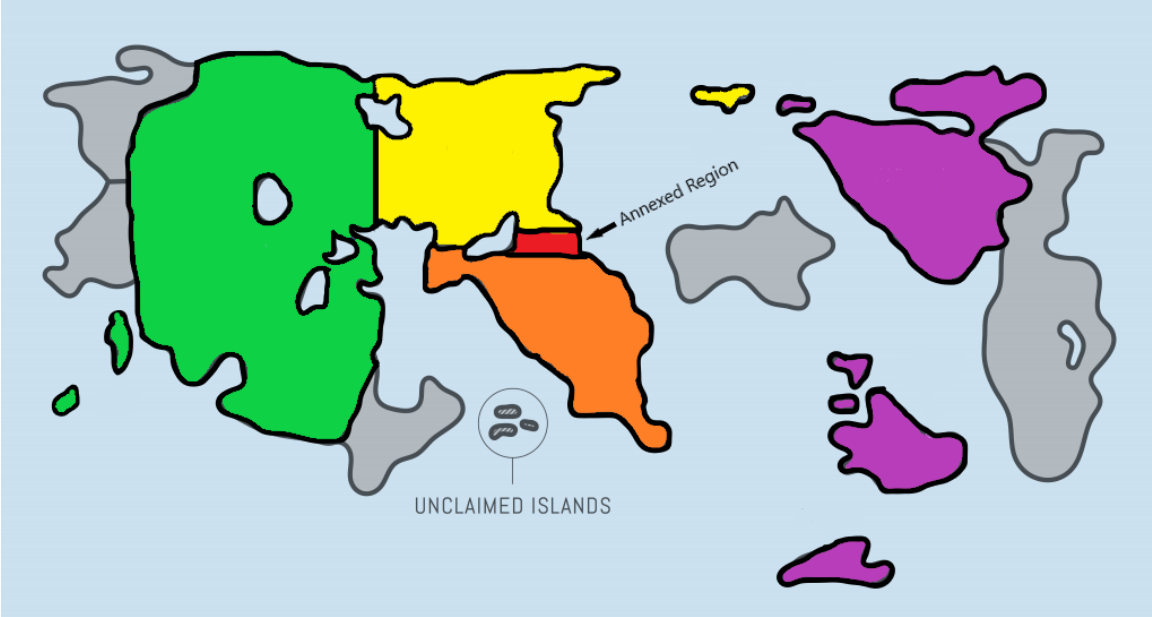
Purple leadership does not want to start a full-scale war with Green, but cannot allow Green to take the islands as it would challenge Purple's position in the region and make allies in the region fear Purple's commitment.

Both Purple and Green's stated policies are that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation. Both states consider unfettered access to and use of its space systems to be a vital national interest.

Purple leadership has asked for recommendations for how to proceed.

Wargaming Scenario 2

Map - All Teams



Purple Team Briefing - Entangled

You work in the ministry of defense for the Kingdom of Purple. Yellow has recently conducted military operations to annex portions of Orange, on their southern border. Orange is not a formal ally with Purple, though they do cooperate with Purple and share common goals in limiting the influence of Yellow in the region. For now, the annexation (depicted in red) is limited to a small segment of the country that is loyal to Yellow due to historical and cultural factors. As a result, Purple has been hesitant to get heavily involved for fear of escalating a war with Yellow. Purple has condemned the incursion, imposed economic sanctions against Yellow, and has begun supplying weapons and money to Orange to counter Yellow's efforts and prevent the annexation from expanding further into the country. Yellow has recently become aware of Purple's efforts and has claimed that Purple is interfering and trying to initiate a proxy war. In response, Yellow has also imposed sanctions and raised the alert status for all of their military forces in the region.

While these events are unfolding, a Purple missile warning satellite that provides coverage over the southern border of Yellow has stopped functioning. Purple military leaders believe the system has been attacked with an offensive cyber weapon in order to obscure further military action in the region, but attribution and confirmation of the attack has not occurred. Purple is currently limited to only ground-based radars for early warning in the region, which means missile warning and missile defense both in the region and in the Purple homeland have been degraded. The lack of early warning has made senior political and military leaders in Purple very nervous. Purple's missile

warning, intelligence, surveillance, and reconnaissance (ISR), and satellite communications (SATCOM) systems support both nuclear/strategic and conventional/tactical missions, so while the tensions with Yellow have not erupted into war, Purple leaders are concerned about the degraded nuclear command, control, and communications (NC3) capabilities as a result of the inoperative missile warning satellite.

Purple's stated policy is that attacks against nuclear command, control, and communication (NC3) systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation for attacks against strategic/nuclear NC3 systems.

Purple Team Briefing - Disentangled

You work in the ministry of defense for the Kingdom of Purple. Yellow has recently conducted military operations to annex portions of Orange, on their southern border. Orange is not a formal ally with Purple, though they do cooperate with Purple and share common goals in limiting the influence of Yellow in the region. For now, the annexation (depicted in red) is limited to a small segment of the country that is loyal to Yellow due to historical and cultural factors. As a result, Purple has been hesitant to get heavily involved for fear of escalating a war with Yellow. Purple has condemned the incursion, imposed economic sanctions against Yellow, and has begun supplying weapons and money to Orange to counter Yellow's efforts and prevent the annexation from expanding further into the country. Yellow has recently become aware of Purple's efforts and has claimed that Purple is interfering and trying to initiate a proxy war. In response, Yellow has also imposed sanctions and raised the alert status for all of their military forces in the region.

While these events are unfolding, a Purple missile warning satellite that provides coverage over the southern border of Yellow has stopped functioning. Purple military leaders believe the system has been attacked with an offensive cyber weapon in order to obscure further military action in the region, but attribution and confirmation of the attack has not occurred. The inoperative satellite performs conventional/tactical warning missions, and purple maintains a separate group of missile warning satellites for strategic/nuclear missions. While strategic nuclear warning remains intact, Purple's ability to monitor activity in the region has been degraded.

Purple's stated policy is that attacks against nuclear command, control, and communication (NC3) systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation for attacks against strategic/nuclear NC3 systems.

Purple Team Briefing - Unknown

You work in the ministry of defense for the Kingdom of Purple. Yellow has recently conducted military operations to annex portions of Orange, on their southern border. Orange is not a formal ally with Purple, though they do cooperate with Purple and share

common goals in limiting the influence of Yellow in the region. For now, the annexation (depicted in red) is limited to a small segment of the country that is loyal to Yellow due to historical and cultural factors. As a result, Purple has been hesitant to get heavily involved for fear of escalating a war with Yellow. Purple has condemned the incursion, imposed economic sanctions against Yellow, and has begun supplying weapons and money to Orange to counter Yellow's efforts and prevent the annexation from expanding further into the country. Yellow has recently become aware of Purple's efforts and has claimed that Purple is interfering and trying to initiate a proxy war. In response, Yellow has also imposed sanctions and raised the alert status for all of their military forces in the region.

While these events are unfolding, a Purple missile warning satellite that provides coverage over the southern border of Yellow has stopped functioning. Purple military leaders believe the system has been attacked with an offensive cyber weapon in order to obscure further military action in the region, but attribution and confirmation of the attack has not occurred. Purple is currently limited to only ground-based radars for early warning in the region, which means missile warning and missile defense both in the region and in the Purple homeland have been degraded. The lack of early warning has made senior political and military leaders in Purple very nervous. While the tensions with Yellow have not erupted into war, Purple leaders are concerned about the degraded nuclear command, control, and communications (NC3) capabilities as a result of the inoperative missile warning satellite.

Yellow Team Briefing - Entangled

You work in the Yellow Department of Defense. Yellow believes that Orange has oppressed people in a northern region of that country who have historical and cultural relationships with Yellow. After a vote of support, Yellow moved military equipment and personnel into the northern region of Orange (depicted in red) to claim it as part of Yellow's sovereign territory. The action was mostly peaceful and is in line with the wishes of the people in the area, despite protests from Orange leadership and the international community. Yellow views the protests as a double standard from colonialist powers and an attempt to limit rightful influence and expansion in the region.

Purple has levied harsh sanctions against Yellow, but Yellow has not escalated the conflict further to draw Purple or Purple's allies into a broader engagement. However, Purple has recently sent shipments of arms as well as provided funding to Orange, so it is clear Purple is attempting to assist in reclaiming the annexed area. Yellow has been forced to raise the alert status of military forces in order to defend against possible efforts by Purple to deploy their own forces to engage in this conflict. Purple uses missile warning, protected SATCOM, and military ISR satellites to monitor and coordinate military actions in the region, so your department considers these systems potential targets to disrupt Purple's ability to monitor your actions as well as coordinate their own responses.

However, Yellow is aware that the missile warning, military ISR, and protected SATCOM systems Purple uses to monitor activity in the region support both their strategic/nuclear missions as well as conventional/tactical missions and are considered critical nuclear command, control, and communication (NC3) assets. Purple's stated policy is that attacks these systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation for attacks against strategic/nuclear NC3 systems.

Yellow Team Briefing - Disentangled

You work in the Yellow Department of Defense. Yellow believes that Orange has oppressed people in a northern region of that country who have historical and cultural relationships with Yellow. After a vote of support, Yellow moved military equipment and personnel into the northern region of Orange (depicted in red) to claim it as part of Yellow's sovereign territory. The action was mostly peaceful and is in line with the wishes of the people in the area, despite protests from Orange leadership and the international community. Yellow views the protests as a double standard from colonialist powers and an attempt to limit rightful influence and expansion in the region.

Purple has levied harsh sanctions against Yellow, but Yellow has not escalated the conflict further to draw Purple or Purple's allies into a broader engagement. However, Purple has recently sent shipments of arms as well as provided funding to Orange, so it is clear Purple is attempting to assist in reclaiming the annexed area. Yellow has been forced to raise the alert status of military forces in order to defend against possible efforts by Purple to deploy their own forces to engage in this conflict. Purple uses missile warning, protected SATCOM, and military ISR satellites to monitor and coordinate military actions in the region, so your department considers these systems legitimate targets potentially to disrupt Purple's ability to monitor your actions as well as coordinate their own responses.

Yellow is aware that the missile warning, military ISR, and protected SATCOM systems Purple uses to monitor activity in the region support both their strategic/nuclear missions as well as conventional/tactical missions, however, Purple has different versions of the systems for each of these missions. The strategic/nuclear versions of the systems are considered critical nuclear command, control, and communication (NC3) assets. Purple's stated policy is to retaliate in a time, domain, and manner of their choosing for any attacks against space systems, up to and including nuclear retaliation for attacks against strategic/nuclear NC3 systems.

Yellow Team Briefing - Unknown

You work in the Yellow Department of Defense. Yellow believes that Orange has oppressed people in a northern region of that country who have historical and cultural relationships with Yellow. After a vote of support, Yellow moved military equipment and personnel into the northern region of Orange (depicted in red) to claim it as part of

Yellow’s sovereign territory. The action was mostly peaceful and is in line with the wishes of the people in the area, despite protests from Orange leadership and the international community. Yellow views the protests as a double standard from colonialist powers and an attempt to limit rightful influence and expansion in the region.

Purple has levied harsh sanctions against Yellow, but Yellow has not escalated the conflict further to draw Purple or Purple’s allies into a broader engagement. However, Purple has recently sent shipments of arms as well as provided funding to Orange, so it is clear Purple is attempting to assist in reclaiming the annexed area. Yellow has been forced to raise the alert status of military forces in order to defend against possible efforts by Purple to deploy their own forces to engage in this conflict. Purple uses missile warning, protected SATCOM, and military ISR satellites to monitor and coordinate military actions in the region, so your department considers these systems legitimate targets potentially to disrupt Purple's ability to monitor your actions as well as coordinate their own responses.

APPENDIX B. WARGAMING DATA

Summary of Actions by Scenario, Treatment, and Wargaming Session

Wargaming Session	Diplomatic, Informational, or Economic	Military Action (Non-space, non-attack)	Military Attack (Non-space)	Space Action (Non-attack)	Space Attack
Scenario 1					
Modeling and Simulation Online Class Spring 2021 (10 teams)					
Entangled (4 teams)	12	14	1	1	6
Disentangled (3 teams)	5	4	2	0	10
Unaware (3 teams)	8	5	2	2	8
Totals	25	23	5	3	24
Modeling and Simulation Class Spring 2022 (12 teams)					
Entangled (4 teams)	12	12	4	0	6
Disentangled (4 teams)	14	10	2	2	4
Unaware (4 teams)	5	6	13	0	12
Totals	31	28	19	2	22
Space Security Class Spring 2022 (12 teams)					
Entangled (6 teams)	30	19	0	0	1
Disentangled (6 teams)	18	16	1	0	16
Totals	48	35	1	0	17
Modeling and Simulation Online Class Spring 2022 (19 teams)					
Entangled (8 teams)	34	19	0	0	7
Disentangled (11 teams)	36	28	5	3	18
Totals	70	47	5	3	25
Scenario 1 Totals (53 teams)	**174**	**133**	**30**	**8**	**88**

Summary of Actions by Scenario, Treatment, and Wargaming Session

Wargaming Session	Diplomatic, Informational, or Economic	Military Action (Non-space, non-attack)	Military Attack (Non-space)	Space Action (Non-attack)	Space Attack
Scenario 2					
Space Security Class Fall 2020 (6 teams)					
Entangled (2 teams)	10	4	0	1	0
Disentangled (2 teams)	9	1	0	0	1
Unaware (2 teams)	8	3	0	2	3
Totals	27	8	0	3	4
Air Force ROTC Fall 2020 (8 teams)					
Entangled (2 teams)	5	3	1	2	5
Disentangled (3 teams)	8	4	0	0	10
Unaware (3 teams)	6	6	2	0	11
Totals	19	13	3	2	26
Modeling and Simulation Class Spring 2021 (7 teams)					
Entangled (2 teams)	9	1	0	0	0
Disentangled (3 teams)	10	3	1	0	3
Unaware (2 teams)	6	4	0	2	7
Totals	25	8	1	2	10
Air Force ROTC Spring 2022 (10 teams)					
Entangled (5 teams)	21	8	2	2	7
Disentangled (5 teams)	19	11	1	1	13
Totals	40	19	3	3	20
Totals (31 teams)	111	48	7	10	60
Overall Totals (84 teams)	**285**	**181**	**37**	**18**	**148**

Summary of Attacks Against NC3 Space Systems by Scenario, Session, and Treatment

Wargaming Session	Kinetic Permanent	Non-kinetic Permanent	Non-Kinetic Reversible	Non-Kinetic Reversible (Localized)	Totals
Scenario 1					
Modeling and Simulation Online Class Spring 2021 (10 teams)*					
Entangled (4 teams)	0	0	1	0	1
Disentangled (3 teams)	1	0	4	0	5
Unaware (3 teams)	2	0	3	0	5
Totals	3	0	8	0	11
Modeling and Simulation Class Spring 2022 (12 teams)					
Entangled (4 teams)	1	0	2	0	3
Disentangled Nuclear (4 teams)	0	0	1	0	1
Disentangled Conventional (4 teams)	0	0	3	0	3
Unaware (4 teams)	1	2	6	0	9
Totals	2	2	12	0	16
Space Security Class Spring 2022 (12 teams)					
Entangled (6 teams)	0	0	0	0	0
Disentangled Nuclear (6 teams)	0	0	0	0	0
Disentangled Conventional (6 teams)	1	1	6	1	9
Totals	1	1	6	1	9
Modeling and Simulation Online Class Spring 2022 (19 teams)					
Entangled (8 teams)	0	0	2	0	2
Disentangled Nuclear (11 teams)	0	0	1	0	1
Disentangled Conventional (11 teams)	1	0	12	0	13
Totals	1	0	15	0	16
Scenario 1 Totals (53 teams)	**6 (7)**	**3**	**37 (41)**	**1**	**47 (52)**

Summary of Attacks Against NC3 Space Systems by Scenario, Session, and Treatment

Wargaming Session	Kinetic Permanent	Non-kinetic Permanent	Non-Kinetic Reversible	Non-Kinetic Reversible (Localized)	Totals
Scenario 2					
Space Security Class Fall 2020 (6 teams)					
Entangled (2 teams)	0	0	0	0	0
Disentangled Nuclear (2 teams	0	0	0	0	0
Disentangled Conventional (2 teams)	0	0	1	0	1
Unaware (2 teams)	0	0	3	0	3
Totals	0	0	4	0	4
Air Force ROTC Fall 2020 (8 teams)					
Entangled (2 teams)	1	0	3	0	4
Disentangled Nuclear (3 teams)	2	0	0	0	2
Disentangled Conventional (3 teams)	1	0	3	1	5
Unaware (3 teams)	3	0	3	0	6
Totals	8	0	9	1	19
Modeling and Simulation Class Spring 2021 (7 teams)					
Entangled (2 teams)	0	0	0	0	0
Disentangled Nuclear (3 teams)	1	0	0	0	1
Disentangled Conventional (3 teams)	1	1	0	0	2
Unaware (2 teams)	2	0	4	0	6
Totals	4	1	4	0	9
Air Force ROTC Spring 2022 (10 teams)					
Entangled (5 teams)	0	0	4	0	4
Disentangled Nuclear (5 teams)	0	0	0	0	0

Disentangled Conventional (5 teams)	1	1	7	0	9
Totals	1	1	11	0	13
Scenario 2 Totals (31 teams)	**12**	**2**	**28**	**1**	**41**
Overall Totals (84 teams)	**18 (19)**	**5**	**65 (69)**	**2**	**90 (95)**

Summary of Attacks Against Other Non-NC3 Space Systems by Scenario, Session, and Treatment

Wargaming Session	Kinetic Permanent	Non-kinetic Permanent	Non-Kinetic Reversible	Non-Kinetic Reversible (Localized)	Totals
Scenario 1					
Modeling and Simulation Online Class Spring 2021 (10 teams)*					
Entangled (4 teams)	1	0	2	2	5
Disentangled (3 teams)	0	0	4	1	5
Unaware (3 teams)	0	0	3	0	3
Totals	1	0	9	3	13
Modeling and Simulation Class Spring 2022 (12 teams)					
Entangled (4 teams)	1	0	2	0	3
Disentangled (4 teams)	0	0	0	0	0
Unaware (4 teams)	0	0	3	0	3
Totals	1	0	5	0	6
Space Security Class Spring 2022 (12 teams)					
Entangled (6 teams)	0	0	0	1	1
Disentangled (6 teams)	0	0	5	2	7
Totals	0	0	5	3	8
Modeling and Simulation Online Class Spring 2022 (19 teams)					
Entangled (8 teams)	0	0	3	2	5
Disentangled (11 teams)	0	0	4	0	4
Totals	0	0	7	2	9
Scenario 1 Totals (53 teams)	**2**	**0**	**26**	**8**	**36**

Summary of Attacks Against Other Non-NC3 Space Systems by Scenario, Session, and Treatment

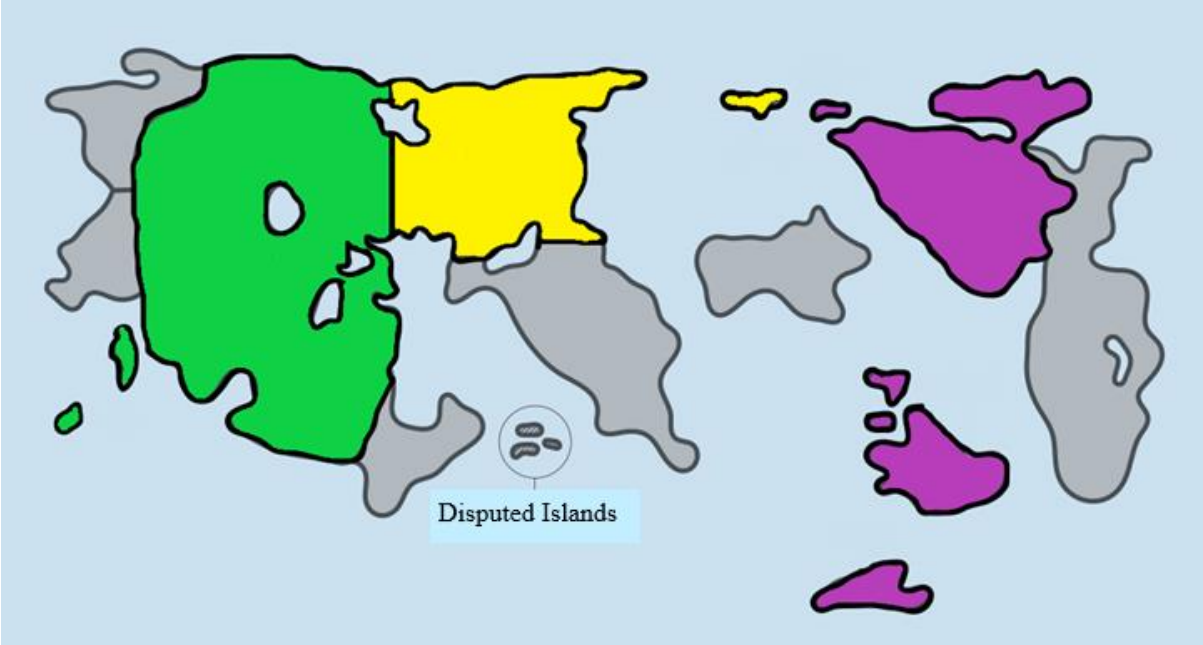
Wargaming Session	Kinetic Permanent	Non-kinetic Permanent	Non-Kinetic Reversible	Non-Kinetic Reversible (Localized)	Totals
Scenario 2					
Space Security Class Fall 2020 (6 teams)					
Entangled (2 teams)	0	0	0	0	0
Disentangled (2 teams	0	0	0	0	0
Unaware (2 teams)	0	0	0	0	0
Totals	0	0	0	0	0
Air Force ROTC Fall 2020 (8 teams)					
Entangled (2 teams)	1	0	0	0	1
Disentangled (3 teams)	1	0	2	0	3
Unaware (3 teams)	2	0	3	0	5
Totals	4	0	5	0	9
Modeling and Simulation Class Spring 2021 (7 teams)					
Entangled (2 teams)	0	0	0	0	0
Disentangled (3 teams)	0	0	0	0	0
Unaware (2 teams)	0	0	1	0	1
Totals	0	0	1	0	1
Air Force ROTC Spring 2022 (10 teams)					
Entangled (5 teams)	0	0	2	1	3
Disentangled (5 teams)	0	0	1	3	4
Totals	0	0	3	4	7
Scenario 2 Totals (31 teams)	**4**	**0**	**9**	**4**	**17**
Overall Totals (84 teams)	**6**	**0**	**35**	**12**	**53**

APPENDIX C. ELITE SURVEY EXPERIMENT

Introduction - All Treatments

You are being asked to complete a survey to examine space security concepts. The survey should take approximately 10 minutes to complete. Although the geopolitical scenario and actors involved are fictional, the background conditions and implications are realistic and plausible. Please read the background information carefully and place yourself in the position of someone who might one day be called upon to make these decisions in the real-world. Short answer responses are optional but highly encouraged/desired. Thank you very much for your time and participation.

Map - All Treatments



Attack Response Table - All Treatments

Type of Attack	Description	Likelihood of Success	Probability of Attribution (Likelihood Purple will know Green carried out the attack)
Kinetic Permanent	An anti-satellite weapon (missile or object in orbit) collides with the adversary satellite and destroys it.	90%	90%
Non-Kinetic Permanent	A laser is used to permanently disable ("blind") an ISR or missile warning sensor.	70%	80%
Non-Kinetic Temporary	A laser is used to temporarily disable ("dazzle") an ISR or missile warning sensor *OR* a communication device is used to temporarily disable (jam) the ability to communicate with a satellite.	90%	80%
Permanent Cyber Attack	A cyberattack is used to permanently disable a satellite on orbit or permanently disable the ability of ground systems to control and communicate with the satellite.	60%	50%
Temporary Cyber Attack	A cyberattack is used to temporarily disable a satellite on orbit or temporarily disable the ability of ground systems to control and communicate with the satellite.	70%	50%

Background - All Treatments

You are a senior space strategist in the Ministry of Defense in the Kingdom of Green. Your country's leaders want to use military force to seize control of disputed islands located in international waters (pictured above). Your peer competitor, Purple, has threatened military intervention if Green attempts to take control of the islands.

Purple's intelligence surveillance, and reconnaissance (ISR) and missile warning satellites provide coverage over the islands and would alert Purple leaders to any of your country's military actions. Additionally, Purple's satellite communications (SATCOM) systems allow forward-deployed military forces to communicate securely with Purple leadership globally.

Some members of your country's leadership believe that attacking Purple's ISR, missile warning, and SATCOM satellites could allow your forces to seize control of the islands without early detection by Purple.

Your country's objectives are limited to gaining control of the islands and do not seek a broader confrontation with Purple.

Additional Background - Entangled Treatment

Purple's ISR, missile warning, and SATCOM systems that could be used to detect/observe Green's campaign and support Purple operations are also part of Purple's nuclear command, control, and communication (NC3) architecture, which provides strategic nuclear warning and missile defense for Purple.

Purple's stated policy is that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation for attacks against NC3 systems.

The Kingdom of Green has the ability to attack space assets using the methods shown in the table below. Your leadership has asked for your recommendation on how to proceed.

Additional Background - Disentangled Treatment

Purple has two sets of ISR, SATCOM, and missile warning satellite systems. One set of satellites supports tactical/conventional missions, like operations to detect and stop Green from taking control of the disputed islands. The other set of satellites is part of their nuclear command, control, and communication (NC3) architecture, which provides strategic nuclear warning and missile defense for Purple. Although it is not its primary mission, the NC3 systems may be capable of providing support for tactical/conventional missions, if needed.

Purple's stated policy is that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation for

attacks against NC3 systems.

The Kingdom of Green has the ability to attack space assets using the methods shown in the table below. Your leadership has asked for your recommendation for how to proceed.

Additional Background - Unknown Treatment

Purple's stated policy is that attacks against space systems will be met with retaliation in a time, domain, and manner of their choosing, up to and including nuclear retaliation.

The Kingdom of Green has the ability to attack space assets using the methods shown in the table below. Your leadership has asked for your recommendation for how to proceed.

Survey Questions:

1. Do you recommend attacks against Purple's missile warning, ISR, and/or SATCOM systems? (If respondent answers no, survey will skip to question 5)
    a. Yes
    b. No

2a. [Entangled/Unknown] Which system(s) would you choose to attack (select all that apply)?
    a. Missile warning (used to detect missile launches)
    b. ISR (used to monitor activity on the ground)
    c. SATCOM (used to enable worldwide communications between leadership and forces)

2b. [Disentangled] Which system(s) would you choose to attack (select all that apply)?
    a. Strategic/nuclear missile warning (used to detect nuclear missile launches and support missile defense)
    b. Tactical/conventional missile warning (used to detect theater/battlefield missiles and warn ground forces)
    c. Strategic/nuclear ISR (used to monitor strategic targets and observe weapons development and launch preparations)
    d. Tactical/conventional ISR (used to monitor military activity on the ground)
    e. Strategic/nuclear SATCOM (used to send nuclear launch codes and strategic messages)
    f. Tactical/conventional SATCOM (used to enable worldwide communications between leadership and forces)

3. Please write a sentence or two explaining your reasoning.

4. Which of the following types of attack are you most likely to employ?
    a. Kinetic permanent/ anti-satellite weapon (using a missile or on-orbit system to destroy the target spacecraft)

b. Non-kinetic permanent (using a laser to permanently blind ISR or missile warning sensors)
c. Non-kinetic temporary (using a laser to temporarily blind ISR or missile warning sensors, or using jammers to disrupt SATCOM systems and/or communications links)
d. Non-kinetic permanent cyber attack (using cyber weapons to disable a target space system or command and control infrastructure)
e. Non-kinetic temporary cyber attack (using cyber weapons to temporarily disable a target space system or command and control infrastructure)

5. Please write a sentence or two explaining your reasoning.

6a. [Entangled] What do you believe Purple's most likely response would be if their ISR, missile warning, and/or SATCOM systems (which are used for NC3 and tactical missions) were attacked?

a. No response
b. Diplomatic condemnation
c. Economic sanctions
d. Cyber attacks to disable Green satellites
e. Missile attacks to destroy Green satellites
f. Military air, land, and/or sea operations against Green's deployed military forces
g. Military air, land, and/or sea operations against Green's homeland
h. Nuclear attack against military capabilities of Green
i. Nuclear attack against major cities in Green

6b. [Disentangled] What do you believe Purple's most likely response would be if their ISR, missile warning, and/or SATCOM systems (which are used for NC3) were attacked?

a. No response
b. Diplomatic condemnation
c. Economic sanctions
d. Cyber attacks to disable Green satellites
e. Missile attacks to destroy Green satellites
f. Military air, land, and/or sea operations against Green's deployed military forces
g. Military air, land, and/or sea operations against Green's homeland
h. Nuclear attack against military capabilities of Green
i. Nuclear attack against major cities in Green

6c. [Disentangled] What do you believe Purple's most likely response would be if their ISR, missile warning, and/or SATCOM systems (which are used for conventional/tactical missions) were attacked?

a. No response
b. Diplomatic condemnation
c. Economic sanctions
d. Cyber attacks to disable Green satellites

e. Missile attacks to destroy Green satellites
f. Military air, land, and/or sea operations against Green's deployed military forces
g. Military air, land, and/or sea operations against Green's homeland
h. Nuclear attack against military capabilities of Green
i. Nuclear attack against major cities in Green

6d. [Unknown Variant] What do you believe Purple's most likely response would be if their ISR, missile warning, and/or SATCOM systems were attacked?

a. No response
b. Diplomatic condemnation
c. Economic sanctions
d. Cyber attacks to disable Green satellites
e. Missile attacks to destroy Green satellites
f. Military air, land, and/or sea operations against Green's deployed military forces
g. Military air, land, and/or sea operations against Green's homeland
h. Nuclear attack against military capabilities of Green
i. Nuclear attack against major cities in Green

7a. [Entangled] Now, imagine that in response to Green's military build-up, Purple carried out attacks on Green's satellite systems. If Green's ISR, missile warning, and/or SATCOM systems (which are used for both NC3 and tactical missions) were attacked, how is Green most likely to respond?

a. No response
b. Diplomatic condemnation
c. Economic sanctions
d. Cyber attacks to disable Purple satellites
e. Missile attacks to destroy Purple satellites
f. Military air, land, and/or sea operations against Purple's deployed military forces
g. Military air, land, and/or sea operations against Purple's homeland
h. Nuclear attack against military capabilities of Purple
i. Nuclear attack against major cities in Purple

7b. [Disentangled] Now, imagine that in response to Green's military build-up, Purple carried out attacks on Green's satellite systems. If Green's ISR, missile warning, and/or SATCOM systems (which are used for Nuclear Command, Control, and Communication (NC3) were attacked, how is Green most likely to respond?

a. No response
b. Diplomatic condemnation
c. Economic sanctions
d. Cyber attacks to disable Purple satellites
e. Missile attacks to destroy Purple satellites
f. Military air, land, and/or sea operations against Purple's deployed military forces

g. Military air, land, and/or sea operations against Purple's homeland
h. Nuclear attack against military capabilities of Purple
i. Nuclear attack against major cities in Purple

7c. [Disentangled] Now, imagine that in response to Green's military build-up, Purple carried out attacks on Green's satellite systems. If Green's ISR, missile warning, and/or SATCOM systems (which are used for tactical missions) were attacked, how is Green most likely to respond?

a. No response
b. Diplomatic condemnation
c. Economic sanctions
d. Cyber attacks to disable Purple satellites
e. Missile attacks to destroy Purple satellites
f. Military air, land, and/or sea operations against Purple's deployed military forces
g. Military air, land, and/or sea operations against Purple's homeland
h. Nuclear attack against military capabilities of Purple
i. Nuclear attack against major cities in Purple

7d. [Unknown] Now, imagine that in response to Green's military build-up, Purple carried out attacks on Green's satellite systems. If Green's ISR, missile warning, and/or SATCOM systems were attacked, how is Green most likely to respond?

a. No response
b. Diplomatic condemnation
c. Economic sanctions
d. Cyber attacks to disable Purple satellites
e. Missile attacks to destroy Purple satellites
f. Military air, land, and/or sea operations against Purple's deployed military forces
g. Military air, land, and/or sea operations against Purple's homeland
h. Nuclear attack against military capabilities of Purple
i. Nuclear attack against major cities in Purple

8a. [Entangled/Disentangled] How credible do you believe it is that Purple would respond to attacks on their NC3 space systems with a nuclear attack (assume the attack crippled NC3 capabilities)?

a. Extremely credible (Purple *would* retaliate with a nuclear attack)
b. Somewhat credible (Purple *might* retaliate with a nuclear attack)
c. Neither credible or un-credible (Purple may or may not retaliate with a nuclear attack)
d. Somewhat un-credible (Purple would probably not retaliate with a nuclear attack)
e. Extremely un-credible (Purple *would not* retaliate with a nuclear attack)

8b. [Unknown] How credible do you believe it is that a state would respond to attacks on their Nuclear, Command, Control, and Communication (NC3) space systems with a nuclear attack (assume the attack crippled NC3 capabilities)?

a. Extremely credible (A state *would* retaliate with a nuclear attack)
b. Somewhat credible (A state *might* retaliate with a nuclear attack)
c. Neither credible or un-credible (A state may or may not retaliate with a nuclear attack)
d. Somewhat un-credible (A state would probably not retaliate with a nuclear attack)
e. Extremely un-credible (A state *would not* retaliate with a nuclear attack)

9. [Treatment Check] Which of the following statements best describes the condition of Purple's space systems in the scenario you were presented (please read carefully)?

a. Purple has ISR, missile warning, and SATCOM systems, but there is no available information about these being part of their nuclear, command, control, and communications (NC3) architecture.
b. Purple has ISR, missile warning, and SATCOM systems that are used for both tactical/conventional missions as well as nuclear/strategic missions, and these systems are part of Purple's NC3 architecture.
c. Purple has two sets of ISR, missile warning, and SATCOM systems. One of which supports tactical/conventional missions, while the other set supports strategic/nuclear missions as part of the NC3 architecture.

10. Do you have any other comments or feedback you'd like to provide?

Demographic Questions for Respondents

11. Do you have experience operating NC3 space systems?

a. No
b. Yes

12. What is your gender?

a. Female
b. Male
c. Other

13. What is your age?

Free Response

14. What is your branch of service?

a. US Army
b. US Navy
c. US Marine Corps
d. US Air Force
e. US Space Force
f. US Coast Guard

g. Other (free response)
h. Not applicable (not in the military)

15. What is the highest grade you have attained?
    a. Junior Enlisted (E1-E4)
    b. NCO (E5-E6)
    c. SNCO (E7-E10)
    d. CGO (O1-O3)
    e. FGO (O4-O6)
    f. GO (O7-O10)
    g. Not applicable (not in the military)

APPENDIX D. PUBLIC SURVEY EXPERIMENT

Introduction - All Treatments

You will read about a hypothetical attack on U.S. satellites. After reading the scenario, you will be asked to recommend a response option.

Initial Attention/Validation Check - All Treatments

It is important to read carefully for this survey. To indicate you are reading carefully, answer "I have a question" below.

a. I understand
b. I do not understand
c. I have a question

Background Briefings

Entangled Kinetic Treatment
A rival country launched a missile attack that destroyed U.S. intelligence and communications satellites. These satellites were also used for nuclear command and control, which enables detection and defense against nuclear attacks against the U.S.

Entangled Non-Kinetic Treatment
A rival country conducted a cyber attack that disabled U.S. intelligence and communications satellites. These satellites were also used for nuclear command and control, which enables detection and defense against nuclear attacks against the U.S.

Disentangled Strategic/Nuclear Kinetic Treatment
A rival country conducted a missile attack that destroyed U.S. intelligence and communications satellites. These satellites are used for nuclear command and control, which enables detection and defense against nuclear attacks against the U.S.

Disentangled Conventional/Tactical Kinetic Treatment
A rival country conducted a missile attack that destroyed U.S. intelligence and communications satellites. These satellites are used for tactical missions only and ARE NOT used for nuclear command and control.

Disentangled Strategic/Nuclear Non-Kinetic Treatment
A rival country conducted a cyber attack that disabled U.S. intelligence and communications satellites. These satellites are used for nuclear command and control, which enables detection and defense against nuclear attacks against the U.S.

Disentangled Strategic/Nuclear Non- Kinetic Treatment

A rival country conducted a cyber attack that disabled U.S. intelligence and communications satellites. These satellites are used for tactical missions only and ARE NOT used for nuclear command and control.

Unknown Kinetic Treatment
A rival country conducted a missile attack that destroyed U.S. military satellites that are used for intelligence collection and communications.

Unknown Non-Kinetic Treatment
A rival country conducted a cyber attack that disabled U.S. military satellites that are used for intelligence collection and communications.

Survey Questions - All Treatments

1. Which of the following response options would you be most supportive of the U.S. taking?
    a. No action
    b. Diplomatic condemnation
    c. Economic sanctions
    d. Cyber attacks to disable rival satellites
    e. Missile attacks to destroy rival satellites
    f. Military air, land, and/or sea operations against rival's deployed military forces
    g. Military air, land, and/or sea operations against rival's homeland
    h. Nuclear attack against military capabilities of rival country
    i. Nuclear attack against major cities in rival country

2. Please write a sentence or two explaining your reasoning.

3. Are the satellites that were attacked used for command and control of nuclear weapons?
    a. Yes
    b. No
    c. This information was not mentioned in the scenario.

4. What is your gender identity?
    a. Female
    b. Male
    c. Other

5. What is your age?
    Free Response

6. What is your race? (Select all that apply)
    a. White
    b. Black or African American

c. American Indian or Alaska Native
e. Hispanic
f. Native Hawaiian or Other Pacific Islander
g. Asian
h. Mixed
i. Other (Fill In)

7. What is the highest level of education you have completed?
   a. Less than high school (Grades 1-8 or no formal schooling)
   b. High school incomplete (Some high school, but no diploma)
   c. High school graduate (or GED certificate)
   d. Some college, no degree
   e. Associate degree
   f. Bachelor's degree (e.g., BS, BA, AB)
   g. Some postgraduate or professional schooling, no postgraduate degree
   h. Postgraduate or professional degree (e.g., MA, MS, JD, PhD, MD

8. In general, would you describe your political views as:
   a. Very liberal
   b. Liberal
   c. Moderate
   d. Conservative
   e. Very Conservative

9. Are you currently serving, or have you ever served, in the United States military?
   a. No
   b. Yes

10. What is your annual household income?
   a. Less than $10,000
   b. $10,000-$24,999
   c. $25,000-$49,999
   d. $50,000-$74,999
   e. $75,000 or more

APPENDIX E. SURVEY STATISTICAL DATA

Elite Sample Summary

Summary Statistics (Combined Regressions)							
	Attack			**Binomial Logit Regression**			
	Yes = 1	No = 0	Chi-Square	Coefficient	Std Error	T value	P-Value
Intercept				0.594	0.596	0.997	0.324
Treatment	32	26	2.15	0.011	0.087	0.127	0.900
Entangled	11	8					
Disentangled	8	11					
Unknown	13	7					
NC3 Experience			0.997	-0.140	0.171	-0.820	0.416
Yes	18	19					
No	13	7					
Gender			1.5	0.223	0.198	1.122	0.267
Male	25	23					
Female	6	3					
Service			3.897	-0.007	0.058	-0.123	0.902
USSF	16	16					
USAF	15	8					
USA	0	1					
RAAF	0	1					
Rank			1.736	-0.048	0.125	-0.384	0.703
NCO	0	1					
CGO	2	3					
FGO	29	22					

Residual Standard Error	0.5121 on 49 df
Multiple R^2	0.05772
Adjusted R^2	-0.03843
F-Statistic	0.6003
P-Value	0.6999

Statistical significance markers: * p<0.1; ** p<0.05; *** p<0.01

Summary Statistics (Individual Regressions)								
Attack Yes =1 No = 0	Coefficient	Std Error	T value	Residual SE	Multiple R^2	Adj R^2	F Stat	P-Value
Treatment				0.501	0.037	0.002	1.058	0.354
Disentangled (Intercept)	0.421	0.115	3.662					
Entangled	0.158	0.163	0.971					
Unknown	0.229	0.161	1.426					
NC3 Experience				0.500	0.029	0.011	1.623	0.208
No (Intercept)	0.650	0.112	5.809					
Yes	-0.178	0.140	-1.274					
Gender				0.496	0.045	0.027	2.551	0.116
Female (Intercept)	0.778	0.165	4.702					
Male	-0.288	0.181	-1.597					
Service				0.499	0.028	0.009	1.501	0.226
USAF (Intercept)	0.652	0.104	6.265					
USAF	-0.168	0.137	-1.225					
USA (Excluded)[376]								
RAAF (Excluded)								
Rank				0.504	0.009	-0.009	0.510	0.470
CGO (Intercept)	0.400	0.225	1.775					
FGO	0.169	0.236	0.714					
NCO (Excluded)								

Statistical significance markers: * p<0.1; ** p<0.05; *** p<0.01

[376] Groups with only one respondent were excluded from regressions due to sparsity effects.

Public Sample Summary

Summary Statistics Overall (Combined Regressions)						
			Logit Regression			
Variable	Chi-Square	F-Test	Coefficient	Std Error	T value	P-Value
Intercept			2.664	0.393	6.782	3.53e-11
Treatment	28.22	1.421	0.114	0.060	1.886	0.060*
Type (Kinetic vs Non)	61.116***	8.555***	0.762	0.128	5.936	5.65e-09***
Gender	2.664	0.329	-0.094	0.133	-0.701	0.484
Age	59.825	1.805*	0.035	0.033	1.061	0.289
Race	36.721	0.992	0.083	0.052	1.597	0.111
Education	32.318	0.575	0.048	0.056	0.872	0.383
Veteran Status	14.058*	1.73*	0.099	0.159	0.627	0.531
Political Views	45.998*	1.776*	0.105	0.056	1.919	0.056*
Income	23.712	0.641	-0.004	0.055	1.919	0.950

Residual Standard Error	1.403
Multiple R^2	0.091
Adjusted R^2	0.074
F-Statistic	5.308
P-Value	6.43E-07

Statistical significance markers: * p<0.1; ** p<0.05; *** p<0.01

Note: These values are affected by the impact of the type of attack on the other variables. Summary statistics separating kinetic and non-kinetic attacks are provided below.

Summary Statistics Kinetic (Combined Regressions)						
			Logit Regression			
	Chi-Square	F-Test	Coefficient	Std Error	T value	P-Value
Intercept			3.545	0.578	6.135	3.87e-09
Treatment	17.223	1.214	0.159	0.096	1.658	0.099*
Gender	8.141	1.014	0.024	0.203	0.119	0.905
Age	47.848	1.205	0.002	0.053	0.039	0.969
Race	36.554	0.807	0.141	0.076	1.854	0.065*
Education	26.434	0.468	0.029	0.083	0.355	0.723
Veteran Status	10.732	1.352	-0.275	0.243	-1.130	0.260
Political Views	36.754	1.842*	0.144	0.085	1.697	0.091*
Income	23.158	0.752	-0.050	0.097	-0.520	0.604

Residual Standard Error	1.490
Multiple R^2	0.044
Adjusted R^2	0.009
F-Statistic	1.273
P-Value	0.259

Statistical significance markers: * p<0.1; ** p<0.05; *** p<0.01

Individual Regressions - Kinetic				
	Coefficient	**Std Error**	**T value**	**P-Value**
Treatment				
Disentangled Tactical (Intercept)	4.039	0.208	19.390	<2e-16
Disentangled Strategic	0.454	0.275	1.651	0.100
Entangled	0.566	0.273	2.074	0.039**
Unknown	0.440	0.299	1.471	0.143
Gender				
Male (Intercept)	4.403	0.165	4.702	<2e-16
Female	0.057	0.196	0.291	0.771
Age				
<=25 (Intercept)	4.182	0.452	9.250	<2e-16
26-30	0.231	0.503	0.459	0.646
31-35	0.265	0.502	0.528	0.598
36-40	0.546	0.495	1.101	0.272
41-45	-0.182	0.529	-0.344	0.731
46-50	0.207	0.574	0.361	0.719
51-55	0.193	0.697	0.277	0.782
56+	0.235	0.546	0.430	0.667
Race				

White (Intercept)	4.322	0.111	38.992	<2e-16
Asian	-0.010	0.388	-0.025	0.980
Black or African American	0.567	0.508	1.116	0.266
Hispanic	0.560	0.377	1.484	0.139
Mixed	0.811	0.340	2.029	0.044**
Other	-0.322	1.491	-0.216	0.829
American Indian or Alaskan	-1.322	1.491	-0.887	0.376
Education				
High School Incomplete (Intercept)	4.375	0.531	8.246	1.22e-14
High School or GED	-0.018	0.665	-0.027	0.979
Some College	-0.214	0.595	-0.359	0.720
Associate Degree	0.534	0.620	0.862	0.390
Bachelor's Degree	0.017	0.547	0.031	0.975
Some Postgrad or Degree	0.125	0.584	0.214	0.831
Political Views				
Very Liberal (Intercept)	4.053	0.242	16.735	<2e-16
Liberal	0.311	0.296	1.051	0.294
Moderate	0.527	0.314	1.824	0.069*
Conservative	0.493	0.331	1.491	0.137
Very Conservative	0.556	0.394	1.410	0.160
Veteran				
No (Intercept)	4.475	0.113	39.766	<2e-16
Yes	-0.064	0.230	-0.278	0.781
Income				
< $10,000	5.000	0.531	9.425	<2e-16
$10,000-$24,999	-0.783	0.616	-1.271	0.205
$25,000-$49,999	-0.588	0.561	-1.049	0.295
$50,000-$74,999	-0.565	0.560	-1.009	0.314
$75,000+	-0.563	0.560	-1.007	0.315

Statistical significance markers: * p<0.1; ** p<0.05; *** p<0.01

For each of the regressions above, additional statistical data is provided below.

Additional Regression Data Kinetic (Individual Regressions)					
	Resid Std Error	**Multiple R^2**	**Adj R^2**	**F Stat**	**P-Value**
Treatment	1.488	0.020	0.007	1.561	0.200
Gender	1.496	0.001	-0.004	0.085	0.771
Age	1.499	0.021	-0.009	0.710	0.664
Race	1.487	0.033	0.008	1.306	0.255
Education	1.501	0.015	-0.007	0.688	0.633
Political Views	1.493	0.017	0.001	1.032	0.391
Veteran	1.497	0.001	-0.004	0.077	0.781
Income	1.500	0.007	-0.010	0.407	0.804

Statistical significance markers: * p<0.1; ** p<0.05; *** p<0.01

Summary Statistics Non-Kinetic (Combined Regressions)						
			Logit Regression			
	Chi-Square	F-Test	Coefficient	Std Error	T value	P-Value
Intercept			2.670	0.527	5.067	7.98e-07
Treatment	31.433	1.286	0.082	0.077	1.059	0.291
Gender	5.542	0.683	-0.223	0.175	-1.268	0.206
Age	54.855	1.23	0.070	0.042	1.650	0.101
Race	46.56	0.787	0.030	0.073	0.410	0.682
Education	45.973	1.091	0.044	0.075	0.593	0.554
Veteran Status	15.509**	1.991**	0.432	0.211	2.045	0.042*
Political Views	39.409	1.025	0.066	0.071	0.926	0.355
Income	23.84	0.38	0.030	0.079	0.375	0.708

Residual Standard Error	1.315
Multiple R^2	0.049
Adjusted R^2	0.017
F-Statistic	1.575
P-Value	0.133

Statistical significance markers: * p<0.1; ** p<0.05; *** p<0.01

Non-Kinetic Individual Regressions				
	Coefficient	**Std Error**	**T value**	**P-Value**
Treatment				
Disentangled Tactical (Intercept)	3.517	0.172	20.079	<2e-16
Disentangled Strategic	0.236	0.238	0.995	0.321
Entangled	0.226	0.237	0.952	0.342
Unknown	0.283	0.246	1.151	0.251
Gender				
Male (Intercept)	3.805	0.106	35.762	<2e-16
Female	-0.217	0.169	-1.287	0.199
Age				
<=25 (Intercept)	4.143	0.287	14.416	<2e-16
26-30	-0.782	0.362	-2.162	0.032**
31-35	-0.431	0.335	-1.288	0.199
36-40	-0.695	0.358	-1.942	0.053*
41-45	-0.506	0.367	-1.378	0.170
46-50	-0.243	0.411	-0.590	0.556
51-55	0.079	0.423	0.188	0.851
56+	-0.276	0.375	-0.737	0.462
Race				

White (Intercept)	3.710	0.098	37.972	<2e-16
Asian	0.157	0.262	0.599	0.550
Black or African American	0.024	0.358	0.066	0.947
Hispanic	-0.293	0.397	-0.738	0.461
Mixed	0.018	0.413	0.043	0.966
American Indian or Alaskan	0.290	0.947	0.307	0.759
Education				
High School Incomplete (Intercept)	3.333	0.537	6.205	2.25e-09
High School or GED	0.897	0.649	1.382	0.168
Some College	-0.031	0.573	-0.054	0.957
Associate Degree	0.406	0.603	0.673	0.502
Bachelor's Degree	0.475	0.548	0.866	0.387
Some Postgrad or Degree	0.400	0.588	0.680	0.497
Political Views				
Very Liberal (Intercept)	3.517	0.244	14.396	<2e-16
Liberal	0.258	0.285	0.904	0.367
Moderate	-0.039	0.291	-0.134	0.894
Conservative	0.313	0.311	1.006	0.315
Very Conservative	0.612	0.340	1.800	0.073*
Veteran				
No (Intercept)	3.608	0.093	38.826	<2e-16
Yes	0.499	0.198	2.517	0.0125**
Income				
< $10,000	3.250	0.331	9.823	<2e-16
$10,000-$24,999	0.434	0.449	0.967	0.335
$25,000-$49,999	0.458	0.359	1.274	0.204
$50,000-$74,999	0.651	0.366	1.779	0.077 *
$75,000+	0.406	0.372	1.092	0.276

Statistical significance markers: * p<0.1; ** p<0.05; *** p<0.01

Summary Statistics Non-Kinetic (Individual Regressions)					
	Resid Std Error	**Multiple R^2**	**Adj R^2**	**F Stat**	**P-Value**
Treatment	1.334	0.006	-0.056	0.533	0.660
Gender	1.320	0.006	0.003	1.657	0.199
Age	1.317	0.039	0.012	1.424	0.196
Race	1.332	0.004	-0.016	0.217	0.955
Education	1.316	0.029	0.010	1.491	0.193
Political Views	1.316	0.025	0.010	1.620	0.170
Veteran	1.311	0.024	0.021	6.335	0.012**
Income	1.323	0.014	-0.002	0.879	0.477

Statistical significance markers: * p<0.1; ** p<0.05; *** p<0.01

ANOVA for Kinetic Treatments

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Disentangled Strategic Kinetic	69	310	4.492754	2.165388
Disentangled Tactical Kinetic	51	206	4.039216	2.398431
Entangled Kinetic	71	327	4.605634	2.442254
Unknown Kinetic	48	215	4.479167	1.744238

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	10.36376	3	3.454587	1.560893	0.199592	2.643014
Within Groups	520.1049	235	2.213212			
Total	530.4686	238				

ANOVA for Non-Kinetic Treatments

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Disentangled Strategic NK	69	259	3.753623	2.276641
Disentangled Tactical NK	58	204	3.517241	1.762855
Entangled NK	70	262	3.742857	1.643064
Unknown NK	60	228	3.8	1.383051

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	2.847059	3	0.94902	0.533245	0.659879	2.640281
Within Groups	450.2658	253	1.779707			
Total	453.1128	256				

ANOVA Comparing Kinetic and Non-Kinetic Treatments

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Kinetic	239	1058	4.426778	2.22886
Non-Kinetic	257	953	3.708171	1.769972

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	63.94878	1	63.94878	32.11803	2.47E-08	3.860352
Within Groups	983.5815	494	1.991056			
Total	1047.53	495				

Welch Two Sample T-Test Kinetic and Non-Kinetic Treatments

Mean Non-kinetic: 3.708

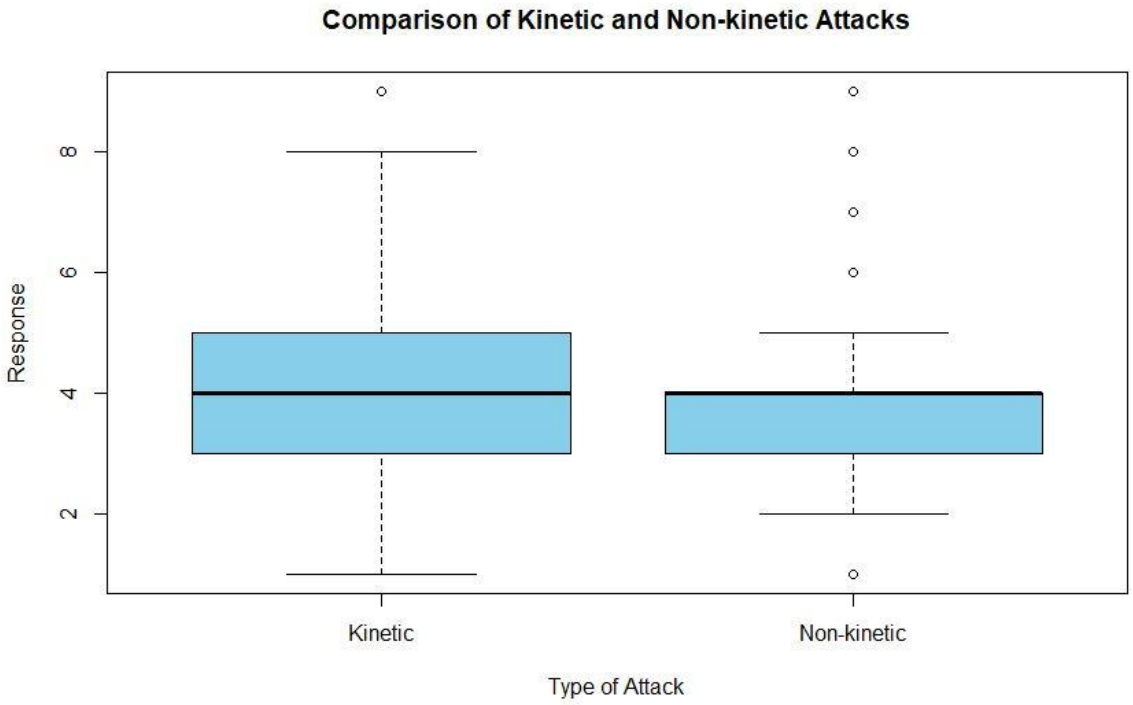
Mean Kinetic: 4.427

T = -5.6437

Df = 477.31

P-Value = 2.858e-08***

Box Plot Comparing Kinetic and Non-Kinetic Treatments



REFERENCES

Acton, J. (2018, February 5). *Command and Control in the Nuclear Posture Review: Right Problem, Wrong Solution.* Retrieved from War on the Rocks: https://warontherocks.com/2018/02/command-and-control-in-the-nuclear-posture-review-right-problem-wrong-solution/

Acton, J. M. (2017). Summary. In J. M. Acton, *Russian and Chinese Perspectives on Non-nuclear Weapons and Nuclear Risks* (pp. 1-94). Washington, D.C. : Carnegie Endowment for International Peace.

Acton, J. M. (2018). Escalation through Entanglement. *International Security*, 56-99.

Acton, J. M. (2020). *Is it a Nuke? Pre-Launch Ambiguity and Inadvertent Escalation.* Washington, D.C.: Carnegie Endowment for International Peace.

Aguinis, H., & Bradley, K. J. (2014). Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies. *Organizational Research Methods*, 351-371.

Air Force Space Command. (2016). *Resiliency and Disaggregated Space Architectures.* Peterson AFB, CO: Air Force Space Command.

Air Force Space Command. (2017, March 22). *Geosynchronous Space Situational Awareness Program.* Retrieved July 01, 2020, from https://www.afspc.af.mil/About-Us/Fact-Sheets/Article/730802/geosynchronous-space-situational-awareness-program-gssap/

Air Force Space Command Public Affairs. (2019, January 4). *Space Flag Prepares Airmen for a Real Fight*. Retrieved from Air Force Space Command: https://www.afspc.af.mil/News/Article-Display/Article/1724474/space-flag-prepares-airmen-for-a-real-fight/

Aldrich, J. H., Gelpi, C., Feaver, P., Reifler, J., & Thompson Sharp, K. (2006). Foreign Policy and the Electoral Connection. *Annual Review of Political Science*, 477-502.

Allison, G. T., & Halperin, M. H. (1972). Bureaucratic Politics: A Paradigm and Some Policy Implications. *World Politics*, 40-79.

Arbatov, A., Dvorkin, V., & Topychkanov, P. (2017). Entanglement as a New Security Threat: A Russian Perspective. In J. M. Acton, *Entanglement* (pp. 11-47). Washington, D.C.: Carnegia Endowment for International Peace.

Barnes, J. E. (2021, September 27). *Intelligence Agencies Pushed to Use More Commercial Satellites*. Retrieved from New York Times: https://www.nytimes.com/2021/09/27/us/politics/intelligence-agencies-commercial-satellites.html

Berinsky, A. J., Huber, G. A., & Lenz, G. S. (2012). Evaluating Online Labor Markets for Experimental Research: Amazon.com's Mechanical Turk. *Political Analysis*, 351-368.

Brzezinski, Z. (1977, September 23). *Memorandum From the President's Assistant for National Security Affairs (Brzezinski) to Secretary of State Vance, Secretary of Defense Brown*. Retrieved from FOREIGN RELATIONS OF THE UNITED STATES, 1977–1980, VOLUME XXVI, ARMS CONTROL AND NONPROLIFERATION: https://history.state.gov/historicaldocuments/frus1977-80v26/d11

Buzhinsky, E. (2009, April 10). *Space: New Combat Theater or Sphere of Cooperation*. Retrieved from Nezavisimoe Voennoe Obozrenie: http://nvo.ng.ru/armament/2009-04-10/1_space.html

Caffrey Jr., M. B. (2019). *On Wargaming: How Wargames Shaped History and How They May Shape the Future.* Newport, RI: Naval War College Press.

Cheng, D. (2012). China's Military Role in Space. *Strategic Studies Quarterly*, 55-77.

Chu, J., & Recchia, S. (2022). Does Public Opinion Affect the Preferences of Foreign Policy Leaders? Experimental Evidence from the UK Parliament. *The Journal of Politics*, 1-4.

Clark, S. (2018, April 15). *It's going to happen: is the world ready for war in space?* Retrieved from The Guardian: https://www.theguardian.com/science/2018/apr/15/its-going-to-happen-is-world-ready-for-war-in-space

Cohen, A. (2010). *The Worst-Kept Secret.* New York, NY: Columbia University Press.

Committee on National Security Space Defense and Protection. (2016). *National Security Space Defense and Protection.* Washington DC: The National Academies Press.

Cunningham, F. S., & Fravel, M. T. (2015). Assuring Assured Retaliation: China's Nuclear Posture and U.S.-China Strategic Stability. *International Security*, 7-50.

Dawson, L. (2018). *War in Space.* Cham, Switzerland: Springer Praxis Books.

Defense Intelligence Agency. (2019). *Challenges to Security in Space.* Washington DC: Defense Intelligence Agency.

Erwin, S. (2017, November 16). *Air Force to discuss "unusual and compelling urgency" for new missile-warning satellites*. Retrieved from Space News: https://spacenews.com/air-force-to-discuss-unusual-and-compelling-urgency-for-new-missile-warning-satellites/

Erwin, S. (2017, November 19). *STRATCOM chief Hyten: 'I will not support buying big satellites that make juicy targets'*. Retrieved from Space News:

https://spacenews.com/stratcom-chief-hyten-i-will-not-support-buying-big-satellites-that-make-juicy-targets/

Erwin, S. (2020, February 10). *Raymond calls out Russia for 'threatening behavior' in outer space*. Retrieved July 11, 2020, from https://spacenews.com/raymond-calls-out-russia-for-threatening-behavior-in-outer-space/

Erwin, S. (2020, September 24). *U.S. Space Command Announces Improvements in Space Debris Tracking*. Retrieved from SpaceNews: https://spacenews.com/u-s-space-command-announces-improvements-in-space-debris-tracking/.

Erwin, S. (2020, March 15). *U.S. Space Force declares 'offensive' communications jammer ready for deployment*. Retrieved from SpaceNews: https://spacenews.com/u-s-space-force-declares-offensive-communications-jammer-ready-for-deployment/

Erwin, S. (2021, April 22). *Lockheed Martin wins $27 million contract modification for integration of DARPA's Blackjack satellites*. Retrieved from Space News: https://spacenews.com/lockheed-martin-wins-27-million-contract-modification-for-integration-of-darpas-blackjack-satellites/

Erwin, S. (2021, September 17). *U.S. Generals planning for a space war they see as all but inevitable*. Retrieved from Space News: https://spacenews.com/u-s-generals-planning-for-a-space-war-they-see-as-all-but-inevitable/

Everstine, B. W. (2021, April 30). *CSO: Space is the 'Wild, Wild West,' Requiring New Norms for Operating in Orbit*. Retrieved from Air Force Magazine: https://www.airforcemag.com/cso-space-is-the-wild-wild-west-requiring-new-norms-for-operating-in-orbit/

Fearon, J. (1994). Political Audiences and the Escalation of International Disputes. *The American Political Science Review*, 577-592.

Fearon, J. (1998). Domestic Politics, Foreign Policy, and Theories of International Relations. *Annual Review of Political Science*, 289-313.

Fearon, J. D. (1995). Rationalist Explanations for War. *International Organization*, 379-414.

Fearon, J. D. (1998). Bargaining, Enforcement, and International Cooperation. *International Organization*, 269-305.

Finch, J. P., & Steene, S. (2011). Finding Space in Deterrence. *Strategic Studies Quarterly*, 10-17.

Friedman, J., Learner, J., & Zeckhauser, R. (2017). Behavioral consequences of probabilistic precision: Experimental evidence from national security professionals. *International Organization*, 803-826.

George, A. L., & Smoke, R. (1974). *Deterrence in American Foreign Policy: Theory and Practice.* New York: Columbia University Press.

George, A. L., & Smoke, R. (1989). Deterrence and Foreign Policy. *World Politics*, 170-182.

Gilpin, R. (1981). *War and Change in World Politics.* Princeton: Princeton University Press.

Glaser, C. (1995). Realists as Optimists: Cooperation as Self-Help. *International Security*, 50-90.

Glaser, C. (2010). *Rational Theory of International Politics.* Princeton: Princeton University Press.

Glaser, C. L., & Kaufman, C. (1998). What is the offense-defense balance and can we measure it? (Offense, Defense, and International Politics). *International Security*, 1-22.

Gohd, C. (2021, November 17). *Russian anti-satellite missile test was the first of its kind*. Retrieved from Space.com: https://www.space.com/russia-anti-satellite-missile-test-first-of-its-kind

Goldman, A., Barnes, J. E., Haberman, M., & Fandos, N. (2020, February 20). *Lawmakers Are Warned That Russia Is Meddling to Re-elect Trump*. Retrieved from The New York Times: https://www.nytimes.com/2020/02/20/us/politics/russian-interference-trump-democrats.html

Government Accountability Office. (2014). *Additional Knowledge Would Better Support Decisions About Disaggregating Large Satellites.* Washnington, D.C.: Government Accountability Office.

Government Accountability Office. (2015). *Defense Satellite Communications: DOD Needs Additional Information to Improve Procurements.* Washington, D.C.: GAO.

Government Accountability Office. (2019). *Space Acquisitions (GAO-19-482T).* Washington D.C.: GAO.

Grey, E. (1925). *Twenty-five Years, 1892-1916.* New York, NY: Frederick A. Stokes Company.

Gruss, M. (2015, July 17). *Maneuvering Russian Satellite Has Everyone's Attention*. Retrieved from Space News: https://spacenews.com/maneuvering-russian-satellite-has-everyones-attention/

Harris, K. (2022, April 18). *Remarks by Vice President Harris on the Ongoing Work to Establish Norms in Space*. Retrieved from The White House:

https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/04/18/remarks-by-vice-president-harris-on-the-ongoing-work-to-establish-norms-in-space/

Harrison, R. G., Jackson, D. R., & Shackleford, C. G. (2009). Space Deterrence: The Delicate Balance of Risk. *Space and Defense*, 1-30.

Harrison, T., Cooper, Z., Johnson, K., & Roberts, T. G. (2017). *Escalation and Deterrence in the Second Space Age.* Washington, DC: Center for Strategic and International Studies.

Harrison, T., Johnson, K., & Roberts, T. G. (2019). *Space Threat Assessment 2019.* Washington DC: Center for Strategic and International Studies.

Harrison, T., Johnson, K., & Young, M. (2021). *Defense Against the Dark Arts in Space.* Washington, D.C.: Center for Strategic and International Studies.

Harrison, T., Johnson, K., Moye, J., & Young, M. (2021). *Space Threat Assessment 2021.* Washington, D.C.: Center for Strategic and International Studies.

Harrison, T., Johnson, K., Roberts, T. G., Way, T., & Young, M. (2020). *Space Threat Assessment 2020.* Washington D.C.: Center for Strategic and International Studies.

Hastings, D. E., & La Tour, P. A. (2016). *An Economic Analysis of Disaggregation of Space Assets: Application to GPS.* Cambridge, MA: Massachusetts Institute of Technology.

Herman, M., Frost, M., & Kurz, R. (2009). *Wargaming for Leaders.* New York, NY: McGraw Hill.

Hill, L. (2019, September 13). *Schriever Wargame Concludes*. Retrieved from Air Force Space Command: https://www.afspc.af.mil/News/Article-Display/Article/1960610/schriever-wargame-concludes/

Holsti, O. R. (2004). *Public Opinion and American Foreign Policy.* Ann Arbor, MI: The University of Michigan Press.

Howell, E. (2022, April 12). *Russia is jamming GPS satellite signals in Ukraine, US Space Force says*. Retrieved from Space.com: https://www.space.com/russia-jamming-gps-signals-ukraine

Hyten, J. E. (2016). *Space Mission Force: Developing Space Warfighters for Tomorrow.* Peterson AFB, CO: Air Force Space Command.

Jervis, R. (1976). *Perception and Misperception in International Politics.* Princeton, NJ: Princeton University Press.

Jervis, R. (1978). Cooperation Under the Security Dilemma. *World Politics*, 167-214.

Jervis, R. (1979). Deterrence Theory Revisited. *World Politics*, 289-324.

Jervis, R. (1993). Arms Control, Stability, and Causes of War. *Political Science Quarterly,* 239-253.

Jervis, R. (1995). Political Implications of Loss Aversion. In B. e. Farnham, *Avoiding Losses/Taking Risks: Prospect Theory and International Conflict* (pp. 187-204). Ann Arbor, MI: University of Michigan Press.

Jervis, R. (2004). The Implications of Prospect Theory for Human Nature and Values. *Political Psychology,* 163-176.

Johnson, K. (2020, September). *Key Governance Issues in Space*. Retrieved from CSIS Aerospace Security Project: https://aerospace.csis.org/wp-content/uploads/2020/09/Johnson_GovernanceInSpace_WEB_FINAL-1.pdf

Johnson-Freese, J. (2017). *Space Warfare in the 21st Century: Arming the Heavens.* New York, NY: Routledge.

Joint Chiefs of Staff. (2020). *Joint Publication 3-14: Space Operations.* Washington, D.C.: Joint Chiefs of Staff.

Jost, T., Meshkin, K., & Schub, R. (2017). Socialized hawks? how selection explains military attitudes on the use of force. *Working Paper*.

Kertzer, J. D. (2020). Re-assessing Elite-Public Gaps in Political Behavior. *American Journal of Political Science*, 1-29.

Kertzer, J. D., & Renshon, J. (2022). Experiments and Surveys on Political Elites. *Annual Review of Political Science,* 1-26.

Kier, E. (1995). Culture and Military Doctrine: France Between the Wars. *International Security*, 65-93.

Kirby, P. (2022, January 12). *Is Russia preparing to invade Ukraine? And other questions*. Retrieved from BBC: https://www.bbc.com/news/world-europe-56720589

Klare, M. T. (2019, November). *Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation*. Retrieved from Arms Control Association: https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation

Klein, J. J. (2006). *Space Warfare: Strategy, Principles, and Policy.* New York, NY: Routledge.

Klein, J. J. (2016, August 30). *Space Warfare: Deterrence, Dissuasion, and the Law of Armed Conflict*. Retrieved from War on the Rocks: https://warontherocks.com/2016/08/space-warfare-deterrence-dissuasion-and-the-law-of-armed-conflict/

Knopf, J. W. (2009). Three Items in One: Deterrence as Concept, Research Program, and Political Issue. In T. Paul, P. M. Morgan, & J. J. Wirtz, *Complex Deterrence* (pp. 31-57). Chicago, IL: The University of Chicago Press.

Knopf, J. W. (2010). The Fourth Wave in Deterrence Research. *Contemporary Security Policy*, 1-33.

Koren, M. (2019, January 11). *The Chill of U.S.-Russia Relations Creeps Into Space*. Retrieved from The Atlantic: https://www.theatlantic.com/science/archive/2019/01/nasa-roscosmos-russia-bridenstine-rogozin/579973/

Krepon, M. (2004). The Stability-Instability Paradox, Misperception, and Escalation Control in South Asia. In M. Krepon, R. W. Jones, & Z. Haider, *Escalation Control and the Nuclear Option in South Asia* (pp. 1-24). Washington, D.C.: The Henry L. Stimson Center.

Krepon, M. (2013, September 16). *Space and nuclear deterrence*. Retrieved from The Space Review.

Kreps, S., & Schneider, J. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics. *Journal of Cybersecurity*, 1-11.

Kroenig, M., & Massa, M. J. (2021). *Are Dual-Capable Weapon Systems Destabilizing? Questioning Nuclear-Conventional Entanglement and Inadvertent Escalation.* Washington, D.C.: Atlantic Council: Scowcroft Center for Strategy and Security.

Lewis, J. A. (2013). Reconsidering Deterrence for Space and Cyberspace. In M. Krepon, & J. Thomspon, *Anti-satellite Weapons, Deterrence, and Sino-American Space Relations* (pp. 61-80). Washington, D.C.: The Henry L. Stimson Center.

Lieber, K. A. (2000). Grasping the Technological Peace: The Offense-Defense Balance and International Security. *International Security*, 71-104.

Lieber, K. A., & Press, D. G. (2006). The End of Mad? The Nuclear Dimension of U.S. Primacy. *International Security*, 7-34.

Lin-Greenberg, E. (2021). Soldiers, Pollsters, and International Crises: Public Opinion and the Military's Advice on the Use of Force. *Foreign Policy Analysis*, 1-12.

Lin-Greenberg, E., Pauly, R. B., & Schneider, J. G. (2022). Wargaming for International Research. *European Journal of International Relations*, 1-45.

List, J. A., & Levitt, S. D. (2005, September 20). *What Do Laboratory Experiments Tell Us About the Real World?* . Retrieved from University of Chicago: http://pricetheory.uchicago.edu/levitt/Papers/LevittList2005.pdf

Lynn III, W. J. (2011). A military strategy for the new space environment. *The Washington Quarterly*, 7-16.

Lynn-Jones, S. M. (1995). Offense-Defense Theory and Its Critics. *Security Studies*, 660-691.

MacDondald, B. W. (2013). Deterrrence and Crisis Stability in Space and Cyberspace. In M. Krepon, & J. Thompson, *Anti-satellite Weapons, Deterrence, and Sino-American Space Relations* (pp. 81-100). Washington, D.C.: The Henry L. Stimson Center.

Mallory, K. (2018). *New Challenges in Cross-Domain Deterrence.* Santa Monica, CA: RAND Corporation.

Manor, M., & Neuman, K. (2009). Air Force Space Command Perspective on Space Deterrence. *Space and Defense* , 37-41.

Manzo, V. (2011). Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit? *National Defense University Strategic Forum*, 1-8.

Mazarr, M. J. (2018). *Understanding Deterrence.* Santa Monica, CA: RAND Corporation.

McClintock, B. (2017). The Russian Space Sector: Adaptation, Retrenchment, and Stagnation. *Space and Defense*, 3-8.

Mearsheimer, J. (2014). *The Tragedy of Great Power Politics.* New York: W.W. Norton and Company.

Mearsheimer, J. J. (1985). *Conventional Deterrence.* Ithaca, NY: Cornell University Press.

Miles, R. (1978). The Origin and Meaning of Miles' Law. *Public Administration Review*, 399-403.

Ministry of Defense of the Russian Federation. (2020, October 20). *Aerospace Forces*. Retrieved from Ministry of Defense of the Russian Federation: https://eng.mil.ru/en/structure/forces/spaceforces/structure.htm

Mintz, A., Redd, S. B., & Vedlitz, A. (2006). Can We Generalize from Student Experiments to the Real World in Political Science, Military Affairs, and International Relations? *Journal of Conflict Resolution*, 757-776.

Moltz, J. C. (2008). *The Politics of Space Security.* Stanford, CA: Stanford University Press.

Moltz, J. C. (2012). *Asia's Space Race.* New York, NY: Columbia University Press.

Moltz, J. C. (2014). *Crowded Orbits.* New York, NY: Columbia University Press.

Morgan, F. E. (2010). *Deterrence and First-Strike Stability in Space.* Santa Monica, CA: RAND Corporation.

Morgan, F. E., McLeod, G., Nixon, M., Lynch, C., & Hura, M. (2018). *Gaming Space: A Game-Theoretic Methodology for Assessing the Deterrent Value of Space Control Options.* Santa Monica, CA: RAND Corporation .

Morgan, F. E., Mueller, K. P., Medeiros, E. S., Pollpeter, K. L., & Cliff, R. (2008). *Dangerous Thresholds: Managing Escalation in the 21st Century.* Santa Monica, CA: RAND Corporation .

Morgan, P. (2019). The Past and Future of Deterrence Theory. In E. Gartze, & J. Lindsay, *Cross-Domain Deterrence* (pp. 51-65). Oxford, UK: Oxford University Press.

Morgan, P. M. (2003). *Deterrence Now.* Cambridge U.K.: Cambridge University Press.

Moscow Bureau. (2022, March 2). *Russia space agency head says satellite hacking would justify war*. Retrieved from Reuters: https://www.reuters.com/world/russia-space-agency-head-says-satellite-hacking-would-justify-war-report-2022-03-02/

Nasu, H. (2022). *Targeting a Satellite: Contrasting Considerations between the Jus ad Bellum and the Jus in Bello.* Newport, RI: Stockton Center for International Law.

National Air and Space Intelligence Center. (2018). *Competing in Space.* Wright-Patterson AFB, OH: NASIC.

National Geospatial-Intelligence Agency. (2020, November 5). *NGA's primary commercial imagery delivery system now includes small satellites*. Retrieved from National Geospatial-Intelligence Agency: https://www.nga.mil/news/NGAs_primary_commercial_imagery_delivery_system_no.html

National Space Society. (2021, December 7). *NSS Statement on Russia ASAT Test*. Retrieved from National Space Society: https://space.nss.org/nss-statement-on-russia-asat-test/

Obama, B. (2010). *National Space Policy of the United States of America.* Washington, D.C.: Office of the President of the United States of America.

Office of the Assistant Secretary of Defense for Homeland Defense and Global Security. (2015). *Space Domain Mission Assurance: A Resilience Taxonomy.* Washington D.C.: U.S. Department of Defense.

Office of the Secretary of Defense. (2018). *Nuclear Posture Review.* Washington D.C.: Office of the Secretary of Defense.

Office of the Secretary of Defense. (2020). *Defense Space Strategy.* Washington, D.C.: Department of Defense.

Office of the Spokesperson. (2021, March 2). *U.S. Sanctions and Other Measures Imposed on Russia in Response to Russia's Use of Chemical Weapons*. Retrieved from U.S. Department of State: https://www.state.gov/u-s-sanctions-and-other-measures-imposed-on-russia-in-response-to-russias-use-of-chemical-weapons/

Perla, P. (1990). *The Art of Wargaming.* Annapolis, MD: United States Naval Institute.

Perla, P. P., & McGrady, E. (2011). Why Wargaming Works. *Naval War College Review*, 111-130.

Perrow, C. (1999). *Normal Accidents.* Princeton, NJ: Princeton University Press.

Pollack, J. (2009). Evaluating Conventional Prompt Global Strike. *Bulletin of the Atomic Scientists*, 13-20.

Posen, B. R. (1991). *Inadvertent Escalation: Conventional War and Nuclear Risks.* Ithaca, NY: Cornell University Press.

Posen, B. R. (1997). U.S. Security in a Nuclear-Armed World. *Security Studies*, 1-31.

Powell, R. (1985). The Theoretical Foundations of Strategic Nuclear Deterrence. *Political Science Quarterly*, 75-96.

Powell, R. (2015). Nuclear Brinkmanship, Limited War, and Military Power. *International Organization*, 589-626.

Press, D. G., Sagan, S. D., & Valentino, B. A. (2013). Atomic Aversion: Experimental Evidence on Taboos, Traditions, and the Non-Use of Nuclear Weapons. *American Political Science Review*, 188-206.

Raju, N. (2021, December 7). *Russia's Anti-Satellite Test Should Lead to a Multilateral Ban*. Retrieved from Stockholm International Peace Research Institute: https://www.sipri.org/commentary/essay/2021/russias-anti-satellite-test-should-lead-multilateral-ban

Rauchaus, R. (2009). Evaluating the Nuclear Peace Hypothesis: A Quantitative Approach. *The Journal of Conflict Resolution*, 258-277.

Raymond, J. W. (2018). *Air Force Space Command Commander's Strategic Intent.* Peterson AFB, CO: Air Force Space Command.

Renshon, J. (2015). Losing face and sinking costs: Experimental evidence on the judgment of political and military leaders. *International Organization*, 659-695.

Rovner, J. (2017). Two kinds of catastrophe: nuclear escalation and protracted war in Asia. *Journal of Strategic Studies*, 696-730.

Rubin, L., Borowitz, M., & Stewart, B. (2020). National Security Implications of Emerging Satellite Technologies. *Orbis*, 515-527.

Russett, B. (1993). *Grasping the Democratic Peace.* Princeton: Princeton University Press.

Russett, B. M. (1963). The Calculus of Deterrence. *Journal of Conflict Resolution*, 97-109.

Saalman, L. (2013). The China Factor. In A. Arbatov, V. Dvorkin, & N. Bubnova, *Missile Defense: Confrontation and Cooperation* (pp. 226-252). Moscow: Carnegie Moscow Center.

Sadat, M., & Sinclair, M. (2021, March 31). *The not-so-secret value of sharing commercial geospatial and open-source information*. Retrieved from The Brookings Institute: https://www.brookings.edu/blog/order-from-chaos/2021/03/31/the-not-so-secret-value-of-sharing-commercial-geospatial-and-open-source-information/

Schelling, T. (1980). *The Strategy of Conflict.* Cambridge, MA: Harvard University Press.

Schelling, T. C. (1966). *Arms and Influence.* New Haven, CT: Yale University Press.

Schneider, J., Schechter, B., & Shaffer, R. (2022). A Lot of Cyber Fizzle But Not A Lot of Bang: Evidence about the Use of Cyber Operations from Wargames. *Journal of Global Security Studies*.

Scowcroft, B. (1976). *Memorandum from the President's Assistant for National Security Affairs to President Ford, April 26, 1976.* Ann Arbor, MI: Ford Library.

Secure World Foundation. (2021, April 3). *Global Counterspace Capabilities*. Retrieved from Secure World Foundation: https://swfound.org/counterspace/

Seligman, L. (2019, December 4). *No One Wins if War Extends Into Space*. Retrieved from Foreign Policy: https://foreignpolicy.com/2019/12/04/thomas-james-interview-space-force-commander-no-one-wins/

Semmel, A. K., & Minix, D. A. (1978). *Small Groups and Foreign Policy Decisionmaking: Some Experimental Findings.* Carlisle Barracks, PA: U.S. Army War College.

Sheffer, L., Loewen, P., Soroka, S., Walgrave, S., & Sheafer, T. (2018). Nonrepresentative representatives: An experimental study of the decision making of elected politicians. *American Political Science Review*, 302-321.

Shelton, W. L. (2017). Threats to Space Assets and Implications for Homeland Security. *Statement Before the House Armed Services Subcommittee on Strategic Forces*, (pp. 1-8). Washington, D.C.

Siddiqi, A. (1997). The Soviet Co-Orbital Anti-Satellite System: A Synopsis. *British Interplanetary Society*, 225-240.

Skillings, J. (2020, December 3). *GPS Rules Everything. And it's getting a big upgrade*. Retrieved from CNET: https://www.cnet.com/features/gps-rules-everything-and-its-getting-a-big-upgrade/.

Smith, R. L. (1976, November 3). *Final Report of the Ad Hoc NSC Space Panel - Part II: U.S.Anti-Satellite Capabilities*. Retrieved from https://aerospace.csis.org/wp-content/uploads/2019/02/Smith-memo-NSC-space-panel-Nov-1976.pdf

Solingen, E. (2007). *Nuclear Logics.* Princeton: Princeton University Press.

Solomone, S. (2013). *China's Strategy in Space.* New York, NY: Springer.

Stares, P. (1985). U.S. and Soviet Military Space Programs: A Comparative Assessment. *Daedalus*, 127-145.

Strout, N. (2020, July 17). *Inside the intelligence community's new plan for commercial imagery*. Retrieved from C4ISRNet: https://www.c4isrnet.com/intel-geoint/2020/07/17/how-the-intelligence-community-is-approaching-commercial-imagery/

Tannenwald, N. (1999). The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use. *International Organization*, 433-468.

Tannenwald, N., & Acton, J. M. (2018). *Meeting the Challenges of the New Nuclear Age.* Cambridge, MA: American Academy of Arts and Sciences.

Taverney, T. D. (2011, August 29). *Resilient, Disaggregated, and Mixed Constellations*. Retrieved from The Space Review: https://www.thespacereview.com/article/1918/1

Tomz, M., Weeks, J. L., & Yarhi-Milo, K. (2020). Public Opinion and Decisions About Military Force in Democracies. *International Organization*, 119-143.

Townsend, B. (2020). Strategic Choice and the Orbital Security Dilemma. *Strategic Studies Quarterly*, 64-90.

Triezenberg, B. L. (2017). *Deterring Space War.* Santa Monica, CA: RAND Corporation.

Trump, D. J. (2017). *National Security Strategy of the United States of America.* Washington D.C.: The White House.

Trump, D. J. (2018). *National Space Strategy.* Washington, D.C.: Office of the President of the United States of America.

Tversky, A., & Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, 453-458.

Tversky, A., & Kahneman, D. (1986). Rational Choice and the Framing of Decisions. *The Journal of Business*, 251-278.

U.S. Department of Commerce. (2020). *Dual-Use Export Licenses*. Retrieved from Bureau of Industry and Security: https://www.bis.doc.gov/index.php/licensing/forms-documents/.../91-cbc-overview

U.S. Space Command. (2020, July 23). *Russia Conducts Space-Based Anti-Satellite Weapons Test*. Retrieved from U.S. Space Command: https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/2285098/russia-conducts-space-based-anti-satellite-weapons-test/

U.S. Space Command Public Affairs Office. (2020, December 16). *Russia tests direct-ascent anti-satellite missile*. Retrieved from United States Space Command: https://www.spacecom.mil/News/Article-Display/Article/2448334/russia-tests-direct-ascent-anti-satellite-missile/

Union of Concerned Scientists. (2021, April 01). *UCS Satellite Database*. Retrieved July 10, 2020, from https://www.ucsusa.org/resources/satellite-database

United States Census Bureau. (2020). *2020 Decennial Census*. Retrieved from American Community Survey 2020 One Year Estimates: https://data.census.gov/cedsci/table?q=United%20States&y=2020

van Evera, S. (1998). Offense, Defense, and the Causes of War. *International Security*, 5-43.

Velkovsky, P., Mohan, J., & Simon, M. (2019, April 3). *Satellite Jamming: A Technology Primer.* Retrieved from On the Radar: https://res.cloudinary.com/csisideaslab/image/upload/v1565982911/on-the-radar/Satellite_Jamming_Primer_FINAL_pdf_bdzxwn.pdf

Waltz, K. N. (1979). *Theory of International Politics.* Reading, MA: Addison-Wesley Publishing.

Waltz, K. N. (2012). Why Iran Should Get the Bomb: Nuclear Balancing Would Mean Stability. *Foreign Affairs*, 2-5.

Watterston, C. J. (2017). Competing interpretations of the stability-instability paradox: the case of the Kargil War. *The Nonproliferation Review*, 83-99.

Weeden, B. (2010). *2007 Anti-Satellite Test Fact Sheet.* Washington, D.C.: Secure World Foundation.

Weeden, B. (2012). *Going Blind: Why America is on the Verge of Losing its Situational Awareness in Space and What Can be Done About it.* Washington, D.C. : Secure World Foundation.

Weeden, B. (2017, October 30). *US Space Policy, Organizational Incentives, and Orbital Debris Removal.* Retrieved from The Space Review: https://www.thespacereview.com/article/3361/1

Weeden, B., & Samson, V. (2019, April 8). *India's ASAT Test is Wake-UpCall for Norms of Behavior in Space*. Retrieved from Space News: https://spacenews.com/op-ed-indias-asat-test-is-wake-up-call-for-norms-of-behavior-in-space/

Weeden, B., & Samson, V. (2021). *Global Counterspace Capabilities.* Washington, D.C.: Secure World Foundation.

Westenhoff, C. M. (2007). *Military Airpower: A Revised Digest of Airpower Opinions and Thoughts.* Maxwell AFB, AL: Air University Press.

Whittington, M. R. (2020, July 19). *Russia rejects joining NASA's Artemis moon program in favor of China*. Retrieved from The Hill: https://thehill.com/opinion/technology/508013-russia-rejects-joining-nasas-artemis-moon-program-in-favor-of-china

Wright, D., Grego, L., & Gronlund, L. (2005). *The Physics of Space Security.* Cambridge, MA: American Academy of Arts and Sciences.

Zak, A. (2016, March 23). *Russia approves its 10-year space strategy*. Retrieved from The Planetary Society: https://www.planetary.org/blogs/guest-blogs/2016/0323-russia-space-budget.html

Zak, A. (2020, February 3). *Everything You Need to Know About Russia's (Possibly Fictional) Super Heavy Rocket*. Retrieved from Popular Mechanics: https://www.popularmechanics.com/space/rockets/a30705512/yenisei-rocket-russia/

Zegart, A. B. (2005). September 11 and the Adaptation Failure of U.S. Intelligence Agencies. *International Security*, 78-111.

Zhang, B. (2011). The Security Dilemma in the U.S.-China Military Space Relationship. *Asian Survey*, 311-332.

Zhang, X., & McClung, S. D. (2010). The Art of Military Discovery: Chinese Air and Space Power Implications for the USAF. *Strategic Studies Quarterly*, 36-62.

Zhao, T., & Bin, L. (2017). The Underappreciated Risks of Entanglement: A Chinese Perspective. In J. Acton, *Entanglement* (pp. 47-76). Washington, D.C.: Carnegie Endowment for International Peace.