2022

Nuclear Deterrence and the Space and Cyber domains

Crook, Matthew R.; Lan, Wenschel D.

Monterey, California: Naval Postgraduate School

NPS-SP-22-012

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

NUCLEAR DETERRENCE AND THE SPACE AND CYBER DOMAINS

by

Matthew R Crook

October 2022

Prepared for: OPNAV N3/N5 – Information, Plans & Strategy. This research is supported by funding from the Naval Postgraduate School, Naval Research Program (PE 0605853N/2098).
NRP Project ID: NPS-22-N052-A

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
		START DATE	END DATE
22-10-2022	Technical Report	01-10-2021	22-10-2022

4. TITLE AND SUBTITLE

Nuclear Deterrence and the Space and Cyber Domains

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
		0605853N/2098
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**
NPS-22-N052-A		

6. AUTHOR(S) Matthew R. Crook

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES.)

Naval Postgraduate School
Space Systems Academic Group
1 University Circle
Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER
NPS-SP-22-012

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES.)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER(S)
Chief of Naval Operations (OPNAV.) N3/N5 – Information, Plans & Strategy	NRP; OPNAV N3/N5	NPS-SP-22-012; NPS-22-N052-A

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release. Distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This study is about how the cyberspace and space domains affect nuclear deterrence. Students at the Naval Postgraduate School in the Space Nuclear Command, Control, and Communications (SNC3) certificate studied this problem as part of their curriculum. They each submitted final papers for the course using their experience, education from the certificate, and research. Their papers are found in the Appendicies of this technical paper. An executive summary and poster also accompany this technical paper.

15. SUBJECT TERMS

Cyber-domain, space-domain, cross-domain, nuclear deterrence, cyber weapons, anti-satellite weapons, nuclear de-escalation

16. SECURITY CLASSIFICATION OF: Unclassified			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	C. THIS PAGE		
Unclassified	Unclassified	Unclassified	UU	92

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER *(Include area code)*
Matthew R Crook	831-656-7703

STANDARD FORM 298 (REV. 5/2020)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Ann E. Rondeau
President

Scott Gartner
Provost

The report entitled "Nuclear Deterrence and the Space and Cyber Domains" was prepared for " OPNAV N3/N5 – Information, Plans & Strategy " and funded by the Naval Postgraduate School, Naval Research Program (PE 0605853N/2098).

Distribution Statement A: Approved for public release. Distribution is unlimited.

This report was prepared by:

_____
Matthew R Crook
Lecturer

Reviewed by:

_____
Prof. James H. Newman, Chair
Space Systems Academic Group

Released by:

_____
Kevin B. Smith
Vice Provost for Research

THIS PAGE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

I. BACKGROUND AND HISTORICAL PERSPECTIVE OF NUCLEAR DETERRENCE AND ESCALATION CONTROL

A. BACKGROUND

It was once said that the three domains of air, land, and sea defined the battlefields of the 20th century, but this is no longer the case in the 21st century. The increased militarization of space and cyberspace has resulted in new warfare domains, which has led to a change in the nature of nuclear deterrence. Before these domains were established, nuclear deterrence was based on the concept of Mutually Assured Destruction (MAD), which is the idea that each nuclear-armed nation would be deterred from attacking another because both would suffer unacceptable levels of damage in retaliation. This concept must be updated in the space and cyber age. The space domain has given rise to new weapons, such as anti-satellite (ASAT) weapons, which can target an adversary's satellites and undermine their ability to communicate and navigate. There are new cyber weapons, such as the Stuxnet worm, used against Iran in 2009.

The emphasis of this paper will revolve around deterrence and escalation strategies, the dilemmas they face in the space and cyber domains, and the complex interactions between them. Many space and cyber assets are dually tasked with conventional and nuclear missions. These domains are newer than the traditional domains, so behavior norms are not well established, and the risk of miscalculation is high. Additionally, actions in the space and cyber domains tend to be covert or unattributable, making it much more difficult for the victim of an attack to interpret an adversary's intentions and formulate a proper, proportioned response.

The paper will endeavor to provide recommendations and answer these five questions:

1. Is US deterrence effective in deterring attacks against the nuclear command and control (NC2) systems via space and cyber vectors?

2. What actions in the space or cyber domains would result in an event significant enough to warrant a US kinetic response, and could they include crossing the nuclear threshold?

3. How can aggression be measured across domains that influence nuclear deterrence and escalation management?

4. What strategies exist to manage escalation and improve deterrence?

5. What is the nuclear threshold in the space and cyber domains, if any?

B. 21ST CENTURY CROSS DOMAIN NUCLEAR DETERRENCE

1. Historic Perspective

The world has learned to live with nuclear weapons over the past 70-plus years. The attacks on Hiroshima and Nagasaki in August of 1945 were burned into the collective global psyche through haunting images of shattered cities and human-shaped silhouettes etched into concrete and buildings. The brutal nature of these weapons and the accompanying fear of their use through deliberate planning or inadvertent escalation has virtually eliminated direct conflict amongst nuclear peers and firmly established strategic deterrence norms. Since 1945 there have been just two instances of direct armed conflict amongst nuclear-armed powers, the 1967 Ussuri River Conflict and the 1999 Kargil War (Brecher, et al. 2021) In both cases, the conflict was minor, resulting in relatively few lives lost, and conducted exclusively via conventional arms in either the land, air, or both domains. Unfortunately, the changing nature of technology, specifically in the cyber and space domains, adds additional friction points to current and future international conflicts. In contrast to the lack of conflict between nuclear-armed powers over the past 70 years, United States (US) intelligence agencies have attributed at least three cyber-attacks from nuclear-armed peers, two from China and one from Russia, in the last decade (Jaikaran 2021) Though these attacks resulted in no lives lost, collectively they impacted millions of people, thousands of companies, multiple US federal agencies, and imposed financial costs. This new trend raises several interesting questions concerning strategic deterrence from a cross-domain perspective.

Where does a cyber-attack trip the line from nuisance to a national security threat? Does a cyber-attack resulting in significant financial losses but not lives lost warrant a discussion on changing strategic deterrence norms? What happens if a cyber or space domain attack impacts a vital Nuclear Command, Control, and Communications (NC3) or Indications, Threats, Warnings, and Assessment (ITWA) capability? Do current deterrence norms provide enough flexibility to be applied across domains to prevent these attacks? Should deterrence in this realm fail, as it clearly has for many years, would a nuclear response be realistic in a situation where attribution cannot be clearly established promptly? This paper seeks to address these questions and provide a framework to analyze the effectiveness of traditional deterrence strategies within the context of a rapidly changing technology landscape. It is first necessary to briefly discuss nuclear deterrence, cyberspace, and the space domain as they relate to national security. Following this brief discussion, a more detailed examination of the mechanisms underpinning deterrence will be utilized to discuss the challenges facing cross-domain deterrence.

2. Unpacking deterrence concepts

Strategy is the art of using all of the resources at one's disposal to alter the opponent's political objectives and perceptions in a way that suits our interests. (Gray, 2010) Deterrence has been called an "exquisite" strategy in that it threatens to use force while not actually using force, to achieve political objectives. This allows for the avoidance of costly military engagements and instead allows for diplomacy to solve international problems. In effect, the purpose of the strategy is to cause the opponent to conclude that the use of violence is not in its best interests.

The current standing policy of the United States is to maintain possession of nuclear weapons to effectively respond to potential adversaries who may seek to do egregious harm. This policy provides a tailored and flexible approach that would ensure unacceptable risks and intolerable costs are imposed. (US Government 2018).

US Nuclear deterrence strategy and policy was developed in the 1950s and 1960s and included concepts such as "Mutually assured destruction" (MAD), a doctrine of military strategy in which a full-scale use of nuclear weapons by two or more opposing sides would cause the complete annihilation of both the attacker and the defender. The strategy is a form of Nash equilibrium (the doctrine is named after the popular 1961 novel by Herman Wouk). Once armed, neither party has any incentive to initiate a conflict or disarm. For decades, this strategy has made uneasy peace between the cold war superpowers. In theory, this strategy would incentivize each side to maintain numerical superiority and disincentivize weapons reduction. Fortunately, cooler heads prevailed, along with the end of the cold war, and both sides significantly reduced the number of warheads from their peak in the mid-1980s.

Since the cold war, deterrence, including nuclear deterrence, has been divided by most scholars into two varieties; deterrence by punishment and deterrence by denial.

a. Deterrence by retaliation (or Deterrence by Punishment)

The deterrence by retaliation strategy is based on the idea that an opponent is less likely to attack if they know they will suffer significant, perhaps intolerable, retribution for doing so. The concept of MAD described above is one extreme example of this strategy. Less extreme examples include economic sanctions, withholding military aid, threatening to remove trade benefits, restricting travel by government officials and their families, imposing tariffs or other trade restrictions, launching cyber attacks, or conventional military attacks.

Strategists generally agree that for nuclear deterrence by punishment to be effective, it must be credible, requires timely execution or survivability, and be transparent.

Credibility means that, in the eye of the potential adversary, the capability and the will exist to carry out the threat. In full view of the world, US nuclear forces carry out tests each year to demonstrate the capability to launch Inter-continental ballistic missiles (ICBMs), submarine launch ballistic missiles (SLBMs), and launch bomber squadrons stills exist and function as designed. These tests are conducted as part of a strategy to demonstrate that the US maintains the capability to carry out nuclear threats against would-be aggressors. The will to carry out the threats is made clear in statements by national leaders and official documents such as the 2018 Nuclear Posture Review and many others.

Timely execution means that, in the eye of the potential adversary, the US can retaliate swiftly enough to launch a counterstrike before US systems can become disabled by a first strike, including a surprise attack.

Survivability means that, in the eye of the potential adversary, the US can retaliate with nuclear weapons even after sustaining a massive attack. Survivability is achieved through the hardening of command and missile locations. In the case of US Ballistic Missile Submarines (SSBNs) through stealth while on alert patrol. In addition to weapons, the Nuclear Command, Control, and Communications (NC3) system Thinline is designed to be survivable in and through a nuclear attack, allowing orders from national leadership to reach launch platforms.

Transparency means that the potential adversary is able to observe enough details about US systems to verify they are a genuine threat. Transparency is the primary reason much information about the US nuclear arsenal is unclassified, where such details would normally be classified for systems with no deterrent function. The need for transparency in nuclear deterrence was famously captured in the movie Dr. Strangelove or: How I learned to Stop Worrying and Love the Bomb. In this fictional story, the Soviet Union develops a doomsday device that will automatically launch a counterstrike on the US if the Soviet Union is attacked by an American nuclear first strike. If it were real, such a device could have the ultimate credibility since its will cannot be in doubt (a machine can only carry out the program for which it was designed), and it could be timely and survivable. In the movie, one US plane without communications (so it could not be recalled by US commanders) manages to penetrate Soviet air defenses and detonate a bomb; this triggers the Soviet Doomsday device. The lesson learned is summarized in a final quote by Dr.

Stragelove "Of course, the whole point of a Doomsday Machine is lost, if you keep it a secret! Why didn't you tell the world, EH?"

b. Deterrence by denial

Deterrence by denial is the concept that, in the perception of the adversary, they would be denied the opportunity or ability to achieve their aims even if they were to attempt it. Like all deterrence strategies, the perception by the potential adversary is the key the success of deterrence by denial. This strategy usually requires robust defensive and security mechanisms to guarantee that even in the most extreme situations, the US nuclear arsenal will maintain enough functionality to launch a retaliatory strike. The US NC3 thinline plays a crucial role in this deterrence method by convincing any potential adversary that an attack on US NC2 to prevent retaliation would most likely fail, and that the US would retain it's ability to retaliate even under to most dire circumstances in a nuclear conflict. While the specific technical details of the US NC3 system should be classified to hide any vulnerabilities, if they exist, at an unclassified level adversaries should understand enough about the US NC3 thinline to know that it has robust protection and redundancy built against attempts at jamming, High-altitude EMPs (HEMPs), nuclear effects, cyber attacks, and so on. If potential adversaires were to falsely believe or perceive the US NC3 thinline to be less robust than it is in reality, this could undermine deterrence by denial. Careful security classification of NC3 thinline specifics should balance the need to protect system technical details and the need for deterrence by denial.

c. The Role of Nuclear Redlines

A nuclear redline is a threshold above which the United States would use nuclear weapons in retaliation for an attack. The purpose of nuclear redlines is to make it clear to potential adversaries that there are limits to what the United States will tolerate and that crossing those lines will result in unacceptable consequences. Redlines provide clarity and certainty to the US nuclear posture, reassuring allies and deterring potential adversaries.

In the past, some nuclear redlines have been fairly straightforward; for instance, an attack on US protected Satellite Communications (SATCOM) used for NC2 would cross a nuclear redline. But with the increased reliance on the Cyber and Space domains in which the fog of war is incredibly thick and the possibility of miscalculation or misunderstanding an adversaries intentions is high, setting redlines in these domains can be fraught with peril.

In the case of a cyber-attack, for example, it may be difficult to attribute the attack to a specific actor with any degree of certainty. This was the case in the Sony hack in 2014 when

the US government attributed the attack to North Korea with a high degree of confidence. Still, many security experts were skeptical of this attribution. (Harris, 2014)

d. The "always/never" Dilemma

This is the idea that nuclear weapons must be under positive control and negative control at all times.

Positive control means that the weapons are always available for use by the proper authority, the President, or their successor in a timely manner. Anything that prevents or unreasonably delays proper leadership from ordering an authorized strike when needed effectively removes positive control. An adversary could defeat positive control by disrupting the communication lines between national leadership and weapon platforms through a kinetic strike or cyber attack. Still, communication lines can also be disrupted by computer glitches or failures, which may have the same effect. Due to the complexity of modern communications systems, it's also not always known whether a failing system is experiencing a self-induced error or interference by an adversary.

Negative control is the idea that nuclear weapons must never be accidentally or by an unauthorized individual or group. US nuclear operators must protect nuclear weapons, control systems, launch codes, and anything else required to launch or order a nuclear launch from access by unauthorized parties and accidents. This requirement means that systems must be protected from both outside and insider threats, which is why many nuclear systems, codes, and procedures require two-person control. The US takes extreme care to guarantee that negative control is always maintained.

There is also a balance between positive and negative control. Anyone who has ever forgotten a password has experienced this. Passwords are meant to guarantee negative control, namely that no unauthorized access will be given except for the individual who knows the password. But if a password is forgotten, then positive control by the authorized individual will have been lost until the password can be reset. So, negative controls must be carefully considered so that they don't remove positive control. Any negative controls that are too cumbersome, take too much time, or are too fragile may be prone to remove positive control. At the same time, too much emphasis on positive control, sometimes referred to as a "hair trigger" posture, may weaken negative control, so a delicate and well-considered balance must be found between these needs. It should be noted that positive and negative control are not necessarily mutually exclusive; they can be guaranteed simultaneously with proper planning, robust and carefully considered procedures

that can be performed quickly and with simplicity by authorized users, but not by unauthorized individuals, and not by accident. The takeaway is that anything meant to strengthen (positive or negative) control must be carefully considered so that it does not detract from the other.

In the context of digital modernization, there are many opportunities to improve the availability and reliability of nuclear systems for authorized users. For instance, modern situational awareness systems such as common operational pictures, intelligence feeds, pictures, and other analyses may be helpful for strategic decision-makers to improve command decision-making.

On the other hand there may also be some liabilities.

3. Cyberspace Trends

"Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures (ITI) including the internet, telecommunication networks, computer systems, and embedded processors and controllers" (New World Encyclopedia 2020) In laymen's terms, cyberspace is the global information network that has reduced the size of the planet, bridged cultural divides, and eliminated untold barriers for billions of people. Unfortunately, it's also a major vulnerability for people, businesses, militaries, and governments around the world. Offensive actions in cyberspace are commonly referred to as cyberattacks, which are defined by the US Government's Computer Security Resources Center (CSRC) as "an attack, via cyberspace, targeting an enterprise's use of cyberspace to disrupt, disable, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" (National Institute of Standards and Technology n.d.) The number of vulnerabilities and attacks within this global domain is staggering. A recent article in Forbes described both the environment and recent attacks (Brooks 2021):

- Projected 55.7 billion connected devices by 2025, with 75% connected to the internet, which will generate 73.1 zettabytes of data
- Distributed denial-of-service (DDOS) attacks will grow to 15.4 million by 2023
- In the first 6 months of 2020, over 26,000 DDOS attacks occurred daily throughout the world

These trends and the underlying vulnerabilities which drive them have received significant attention from the US Government. President Trump issued the first "fully articulated cyber strategy in 15 years" in September of 2018 (The Office of the President of the United States 2018, 1). One of President Biden's early presidential actions was the "Executive Order on Improving the

Nation's Cyber Security" issued on May 12, 2021. Both documents sought to drive the whole of the government's efforts to enhance the US's cyber defense/security posture to preserve capacity and limit societal or government impact from all cyber actors. Though the Trump era document has been relegated to the back burner by the new administration, the general trends of the Trump era document are largely preserved, concrete actions are specified, and responsibilities are assigned to specific agencies within the Biden document. As this environment continues to mature, its influence on military and national strategies is expected to grow significantly.

4. Deterrence in the Cyber Domain

The increased complexity of digital systems can have a negative impact on nuclear deterrence. Cyber systems can undermine deterrence, and actions by another nation can be easily misunderstood. Additionally, improvements in nuclear control systems capabilities that enhance the reliability of nuclear operations might improve the credibility of threats, assuming that information about improvements can be shared with the targets of the threats. However, the increased complexity of digital systems can also lead to misunderstandings and accidental escalation. Actors who want to assess the reliability of complex nuclear control systems will need ever more intelligence, and active penetration of digital systems for intelligence also opens the possibility of manipulating the data in the functionality of the same systems.

While many people attempt to draw similarities between the cyber and nuclear domains, in reality, they are quite different in many ways, and it may be useful to contrast them for clarity.

While nuclear weapons create severe irreversible damage, cyber weapons do not create immediate and devastating consequences. Additionally, most cyber operations are conducted over a long period of time, where they can collect information that may be used to support other domains or to justify other types of actions.

Cyber weapons, when employed by governments, are generally used for one of four categories, intelligence gathering, information campaigns used to influence the populace or target group, disruption of critical infrastructure (which would presumably cause disruption of operations that depend on that infrastructure), or destruction of data or systems. Ransomware is one example of a cyber weapon, where cyber criminals steal data and encrypt it so that the data cannot be accessed. However, this type of weapon, which may be useful to criminals, has almost never been used by governments.

Governments seeking to use cyber weapons to gather intelligence do so covertly and over a long period of time. Users of these weapons use extreme care to avoid detection, and this also means that attributing the source of the attack is difficult. These weapons could be employed in an effort to gain information about the nuclear command, control, and communications systems. Ironically, if the attacker gained intelligence that verified capabilities that are threatened for nuclear deterrence purposes it could add to the credibility of the deterrence system, but this is an unusual case. Also possible is that an intruder intending only to gain information could unintentionally damage or destroy data that is essential to the nuclear command and control system, or if discovered, the intentions of the intruder may not be properly understood by the victim, which could then generate a response that is wholly disproportionate to the situation.

Information campaigns while interesting are beyond the scope of this technical paper, so they will not be discussed further.

The final two categories, weapons to disrupt or destroy critical infrastructure could theoretically be used against critical nuclear facilities, communication links, or warning systems.

One unique aspect of cyber warfare is that each of the categories above requires exploiting a vulnerability that, in most cases, the victim is not aware of. For this reason, it would be very difficult to use cyber warfare as a deterrent in the way that other weapons can be used. As stated earlier deterrence requires transparency and credibility. Revealing the existence of a cyber weapon would, in most cases, reveal the vulnerability that it exploits. Once a vulnerability has been revealed the system owner would rush to fix it, and in most cases, vulnerabilities are easier to fix than the cyber weapon. While not true of all cyber weapons, many cyber weapons can only be used once, or for a very short time, since their use will alert the victim to their existence and typically the vulnerability.

(Finish thought here, that cyber weapons are no good for deterring action (in most cases) – but may interact with nuclear deterrence.

There are limited ways in which cyber weapons can cause actual destruction, but there are examples of this also. The Stuxnet virus was designed to damage the Iranian nuclear program, specifically targeting uranium enrichment centrifuges.

5. Space Domain Trends

Currently, the role of the space domain is primarily relegated to support or enablement of terrestrial operations. These include theater and global communications, weather, navigation, timing, and threat warning. (United States Space Force, 2022) Though governments were the first organizations to use the space domain, the commercial space sector is far more extensive and just as complex as their government counterparts. As of May 1st 2022 the makeup of operational satellites in orbit is as shown in Table 1 & 2 to the right. (Union of Concerned Scientists, 2022)

Total Operating Satellites	5465	
United States	3433	63%
Russia	172	3%
China	541	10%
Other	1319	24%

Table 1- Worldwide Satellites by Nation

United States Satellites	3433	
Civil	31	1%
Government (non-DoD)	172	5%
Military	237	7%
Commercial (except Starlink)	1292	38%
Starlink	1700	50%

Table 2- United States Satellites by Sector

Note that the United States alone operates more than half of the world's satellites, and in the short-term this number will grow as the SpaceX Starlink constellation is populated.

Like the cyber domain, space has become a highly contested. According to one Space Force General, "American satellites are attacked by adversaries every day in ways that flirt with acts of war…" (O'Neill, 2021) These sentiments are echoed in more formal US government documents to including the 2020 Defense Space Strategy. This document highlights the central problem facing this domain succinctly, "The US Defense space enterprise was not built for the current strategic environment. The intentions and advancements of potential adversaries in space are threatening the ability of the United States to deter aggression, protect US national interests, and to fight and win future conflicts" (Defense, 2020). Many new technologies are increasingly leveraging the unique attributes of space and its associated satellites to enable terrestrial capabilities. As this trend continues, disruptions in space-based assets are becoming more problematic and impacting an ever-growing range of abilities and services, which further complicates the deterrence landscape.

6. Cross-Domain Considerations: The impact of Cyber and Space domains on Nuclear Deterrence

The first successful US military satellite briefly entered orbit in January of 1958, and the first US military communications satellite was launched in December of that same year. (NASA Jet Propulsion Laboratory, 2022) The counter-response to this feat was swift. The first US anti-satellite weapon was tested in October 1959, and the Soviet Union tested its system in 1963. (George, 2019) This counter capability saw slow but steady growth during much of the Cold War. The early 2000s witnessed a reinvigoration of threats within the space domain with the introduction of newer and more capable missiles, lasers, and research into directed-energy weapons. (Ibid) The investment into these weapons follows a pattern of behavior designed to exploit US dependencies on space with the intent of contesting or denying US access to and operations in this domain. (Defense, 2020)

The first real cyber-attack is attributed to the Morris Word, a Denial-of-service attack, which impacted approximately 6,000 computers, or roughly 10% of computers connected to the internet at the time (La Trobe University, 2022). As the number of computers connected to the internet has continued to increase, the cyber surface area vulnerable to attacks has increased. Because of this growth, attacks have increased in frequency, complexity, and severity. What's more, these attacks are increasingly the acts of state actors, whether in uniform or not. A recent US intelligence agency's annual threat assessment states, "Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves and in some cases can demonstrate its ability to damage infrastructure during a crisis." (Office of the Director of National Intelligence, 2021)

7. Cross-Domain Dependencies

The preceding sections describe the three areas as separate entities for ease of explanation. However, the reality is far more complicated. Space-based assets have been an integral part of deterrence for decades. The ultimate highground enables effective nuclear Command, Control, and Communications (NC3) comprised of the Integrated Tactical Warning and Attack Assessment (ITW/AA), US Nuclear Detonation Detection System (USNDS), communications system satellites, and NC3 related mission payloads (US Department of Defense, 2020) As the name suggests, NC3 focuses on the command and control of US nuclear forces at all times, even under the enormous strain of nuclear attack (Ibid). Though NC3 consists of more than space-based assets, satellites play an outsized role in the NC3 construct due to the advantages offered by their operational domain.

Attacks impacting this portion of the NC3 portfolio can easily be misinterpreted as adversary attempts to gain an advantage during a crisis. Regardless of the attack type, intentional or even inadvertent, targeting of satellites supports NC3, or ITW/AA may be understood as an attempt to gain a first strike advantage. The degree to which specific impacted systems support nuclear operations creates a significant degree of uncertainty in a highly volatile situation.

The cyber domain's impact on nuclear operations is more difficult to assess at this classification level due to the security surrounding NC3 connections, defenses in place, as well as the nature and age of many components of the US strategic deterrence portfolio. Due to the absolute requirement of uninterrupted service during a nuclear crisis, any cyber-attack which results in detriments to NC3 connectivity could be viewed in a similar vein as attacks against satellite enabled capabilities of NC3. To date, many nuclear capabilities have enjoyed an ironic form of cyber protection due to the underfunding of the nuclear enterprise, outdated and isolated systems. As the US nuclear enterprise undergoes a near total platform update, cyber protection must be incorporated from the very beginning.

It's clear that space plays an integral role in effective nuclear command and control and is, therefore a requirement of nuclear deterrence. Cyberspace's contribution to nuclear deterrence is somewhat unclear. The 2018 NPR makes numerous references to cyber as a general threat vector but does not mention improving cyber as part of or an enabler of the nation's nuclear deterrence construct. Accordingly, this paper will address space-based threats as both general and specific threats, while cyber-based threats will be considered general threats only.

8. Deterrence Across Domains

The essence of nuclear deterrence, as stated previously, is that it deters existential threats due to the promise of assured destruction. New challenges in the cyber and space domain are testing the applicability of nuclear deterrence and, potentially, its associated existential litmus test. Threats that fall below the existential litmus test do not fall under a nuclear deterrence strategy since a nuclear response is inappropriate for the situation. Many examples of threats were not existential to the US over the past 70 years. For instance, despite the US's nuclear monopoly, in 1949, the Soviets surrounded and cut off Berlin for over a year, resulting in the Berlin Airlift and the first major post-WWII conflict between the US and Soviet Union. A few years later, the North Koreans, and later the Chinese, invaded South Korea while bereft of their own nuclear weapons. This pattern was repeated in multiple incidents and includes two examples of dyadic nuclear pairs engaging in limited, non-existential conflicts without nuclear weapons.

Given the centrality of the concept of existential threats to these scenarios, it may be essential to define what is meant by the term. Existential threats are those threats that challenge the continued existence of an organization or group of people. The time scale of an existential threat is variable and depends upon the means available to the antagonist. For example, the Nazi treatment of the Jewish people during WWII represented an existential threat to that community, which took place over several years. The Cold War, with its many thousands of nuclear warheads, represented an immediate existential threat to both individual nations and humanity in the event of unconstrained nuclear warfare.

II. CURRENT THREATS

A. CURRENT CYBER AND SPACE THREATS TO NUCLEAR DETERRENCE

1. Complications to nuclear deterrence that stem from the cyber domain

Of the two domains, the more consistent threat lies in cyberspace. The trendlines mentioned above strongly suggest that interconnection enabled via cyberspace will continue to grow for the foreseeable future, which means the threat surface area from this domain will also expand. Severe challenges exist when discussing cross-domain deterrence from a nuclear perspective within this domain. First, where is cyberspace's existential tipping point, or nuclear threshold? A brief review of the many cyber-attacks compiled by the Center for Strategic and International Studies (CSIS) listed multiple examples of denials of service, espionage, MALWARE insertions, and financial losses, but no significant power outages, runaway nuclear power plants, or particularly dangerous activities (Center for Strategic & International Studies, 2022). Second, what is the ability to correctly attribute cyber-attacks? How does the proliferation of Virtual Private Networks (VPNs), multiple routing pathways, and public internet access points or computers impact cyber response attribution? In short, can deterrence, nuclear or otherwise, be effective when the identity of cyber actors may not be known? Third, assuming attribution is possible, what element of the cyber actor's country represents a legitimate counter-target? Or, what if the responsible party is not a state actor? Fourth, what does a nuclear response, or nuclear deterrent threat, look like in terms of proportionality? Answering these questions is critical in determining whether nuclear weapons would be applicable, let alone compelling, in this domain.

Determining whether an attack from cyberspace could pose an existential threat to the US is incredibly difficult as it depends on many variables and is likely classified. Using publicly available data from the Director of National Intelligence for the US, cyber actors do not currently appear to pose an existential threat to the US (Office of the Director of National Intelligence, 2021). Table 3 summarizes the modern cyber threats presented in the report from the US's four primary adversarial nations: China, Russia, Iran, and North Korea. In addition to the information in Table 3, various news

Table 2- Adversary Nations Cyber Capabilities, derived from the DNI's 2021 Annual Threat Assessment

Nation	Current Assessment	Notable Capabilities
China	Prolific // Low-Level	Espionage; influence threat Cyber-attacks capable of localized, temporary disruptions to critical infrastructure
Russia	Top Cyber Threat	Espionage; influence; attack Cyber-attacks capable of disrupting and damaging infrastructure
Iran	Significant Threat	Espionage; influence, attack Cyber-attacks capable of short-term effects
North Korea	Growing threat	Espionage; theft; attack Cyber-attacks capable of temporary, limited disruptions of some critical infrastructure and business networks

reports on cyber-attacks have not mentioned excessive fatalities or significant disruptions to civil infrastructure. The first fatalities associated with a cyber-attack were only reported in the past few years, and these deaths were clearly an unintended side effect (Eddy and Perlroth 2020) At this point in time, the available data strongly suggests that cyberattacks do not pose an existential threat to the US government, the American people, or their way of life.

Attribution is the new major challenge that must be addressed when considering a potential cross-domain response or deterrence posture. Unfortunately, cyber attribution can be very challenging depending on the sophistication of both the attacker and defender, the attacker's motivation, the involvement of multiple victims, and numerous other variables. In a select few situations, attribution assessments have been made relatively quickly. The CSIS's partial list of Cyber Attacks since 2006 contains several entries with attribution statements, including the following (Center for Strategic & International Studies, 2022):

- February 2022 – Distributed Denial of Service (DDoS) against Ukrainian Defense Ministry and several banks – US and UK attributed the attack to the Russian GRU
- February 2022 – Malware attack against Palestinian individuals and organizations – Researchers suggest operation could be connected cyber arm of Hamas
- August 2021 – Hacks against Israel government and tech companies – originally attributed to Iran but later assessed to have been Chinese in origin

Unhappily, it appears attribution is the exception as opposed to the norm. The CSIS list contains hundreds of attacks spanning almost two decades, but only seven attribution statements, of which several indicate uncertainty or were proven incorrect upon further investigation. In short, though incredibly important for both response and deterrence considerations, at this point, attack attribution is not guaranteed to be correct or timely.

Assuming a non-existential threat cyber-attack was correctly attributed to an actor, what does an appropriate response entail? If a significant amount of wealth is destroyed, is a military response of any kind warranted? How many lives, if any, are worth that amount of money? In 2009 Bernie Maddoff plead guilty to the largest private Ponzi scheme in history, which decimated the savings of 37,000 people across 136 countries of as much as $65 billion dollars

(Steinberg, 2021) In contrast, the CSIS list of Significant Cyber Crimes only lists five cyber-attacks with an economic impact in the multi-million-dollar range, with the largest impact totaling approximately $50 million dollars. Bernie Maddoff was ultimately sentenced to life in prison and ordered to pay restitution. Financial crimes are not the same as cyber-attacks, despite the high dollar cost of these acts. The outcome of the Maddoff situation begs the obvious question, if a $65 billion crime results in life in prison and a fine, is it realistic to view similar-sized cyber-attacks as acts of war? Given cyber-attacks' lack of fatalities and generally short-term impacts, military kinetic responses are not warranted.

If a major cyber-attack is successfully attributed and deemed serious enough to warrant a kinetic response, what portion of an adversary's nation is a legitimate target? Given current western thoughts on the value of life and limited warfare, the most likely response would be some sort of stand-off attack. However, this is clearly a traditional act of war and fraught with a degree of mission risk (the missile could be shot down, malfunction, or miss the target) and an even higher conflict escalation risk. Looking beyond the means, the target itself would likely be challenging to select. Attacking the building where the attack originated would likely not stop future cyber-attacks as buildings are generally resilient, communications systems able to access the internet are ubiquitous, and the people behind the attack may or may not be present at the time of the strike. Finally, what if the attack originated from cyber-actors located in neutral third country? International norms do not support attacks within a neutral nation's borders due to the actions of foreign non-state actors.

The preceding paragraphs focused on a nuclear cross-domain response, but their tenets also apply to deterrence applications as well. Cyber-actors who've acted with virtual immunity for the past 10 or 20 years, will not be impacted by attempts at nuclear brinksmanship or deterrent messaging. The same issues which stymy a nuclear response are operative on the deterrence side of the equation as well and directly impact the credibility of nuclear threats.

It seems clear that cross domain nuclear deterrence or an actual nuclear response to a cyber-attack could only be justified if the attack poses an existential threat to the U.S. NC3 thinline or other essential nuclear systems. Ther remainder of this technical paper will assume that any cyber or space domain attack may disable U.S. nuclear systems, or in some way pose an existential threat to the U.S. government, or citizens.

2. Deterrence in the Space Domain

Space-based threats represent a different, but still similar, threat to the US, its interests, and allies. To date, space-based threats have been limited to disrupting US space-based systems as opposed to delivering terrestrial effects from space (Rods from God, nuclear warheads released from a satellite, or other similar type concepts). These disruptions include both kinetic and non-kinetic attacks designed to deprive the US of its asymmetric advantages provided by its space-based platforms. Figure 1 provides the current threat spectrum confronting the US in space (Defense, 2020). Somewhat surprisingly, threats to space-based systems share many of the same attributes as attacks via cyberspace. First, threats to these platforms are clearly extensive, but they are not existential in nature. Losing one, ten, or all US satellites will not cause US society to fail, though many modern-day convieniences would be serverely impacted. Second, destroying a satellite does not typically cause a loss of life, which makes consideration of a nuclear response challenging in terms of proportionality. Third, there may be attribution challenges, depending on the attack vector.

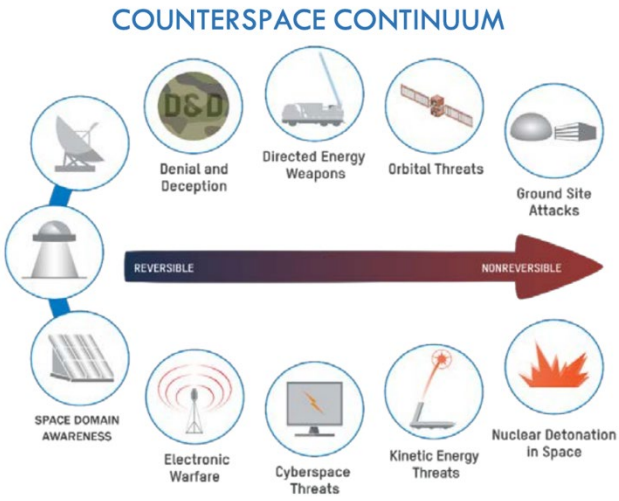


Figure 1 - Threats to Space based platforms

Destroying, or otherwise rendering inoperable, a satellite in space is clearly not an existential threat. First, satellites have become a part of daily life, but as of now very few individuals rely on a satellite to the extent that its loss would cause them irreparable harm. This applies to both individuals, corporations (satellite centered companies excluded), and most government functions. This is not to say that losing satellites wouldn't be painful or economically damaging. Second, almost all satellites are part of a broader constellation, so destroying a single, or even a small number of, satellites would likely not render the entire constellation inoperable. Third, most critical government satellites are in higher orbits which makes physically attacking them more difficult. Given these facts, it's clear utilizing nuclear weapons to prevent, or respond to, actions in this domain is not a credible threat.

One possible exception to this conclusion would be the destruction, or significant disruption, of satellites comprising the US's NC3 system. These satellites are involved with either the ITW/AA, Nuclear C2, or nuclear event detection that their destruction or incapacitation could justifiably be seen as a preemptive nuclear attack. If either of these functions is rendered ineffective due to an attack, it could be construed as an attempt to generate a first strike advantage. Depending on the timing of the event and status of nuclear forces around the globe at the time, this could be incredibly dangerous. It's impossible to predict with accuracy where this could drive a conflict, other than to say it would clearly escalate the situation and increase the possibility of inadvertently crossing a nuclear threshold.

Assuming a nuclear red line was not crossed, the next issue to consider is attack attribution. Though attribution is generally considered easier than in cyberspace, challenges could remain. Sensors can detect, track, and assess the origin location of most counter satellite missiles, at least well enough to provide a country of origin. Since anti-satellite weapons are not common amongst most militaries, "close enough" counts in this context. The 2021 Global Counterspace Capabilities is an exhaustive report which details every counterspace system across the globe. According to the report, just eight nations possess any counterspace capabilities (Secure World Foundation 2021, xv-xvii) On orbit threats, as depicted in Figure 1, can also generally be tracked as well and only three nations possess this operational capability (Secure World Foundation 2021, xv-xvii) In a similar vein, directed energy and electronic warfare attacks present attribution challenge, but again are limited to same three nations (Secure World Foundation 2021, xv-xvii) Considered holistically, attribution in space is less of an issue than in cyberspace.

Assuming correct attribution, the concept of proportionality remains a problem. Threatening to use a nuclear weapon in response to a destroyed satellite, or the shutdown of a power grid for a few hours, is simply not a proportional response and thus not a credible threat.

III. THE FUTURE OF NUCLEAR DETERRENCE

A. WHAT ACTIONS IN THE CYBER OR SPACE DOMAINS REQUIRE A RESPONSE, AND UNDER WHAT CONDITIONS COULD A NUCLEAR RESPONSE BE WARRANTED?

As already discussed a nuclear response to an attack in the cyber or space domain would be difficult, if not impossible, to justify unless the attack specifically denied or destroyed systems which are used for nuclear deterrence such as US early warning systems, and NC3 thinline communications, or somehow posed an existential threat to the lives of the people of the USA or to continued operation of the government. This is an exceptionally high standard, and there are very few situations that could produce such a threat.

As the US already does with Russia, nuclear redlines should be draw around any system that is used for US early warning or NC3 thinline communications.

How to define nuclear redlines in the cyber domain can be especially precarious since drawing redlines also highlights which systems are vital to NC2. There may be systems which play a role in NC2 that adversaries are not fully aware of.

If US nuclear systems, including NC2 are not vulnerable to cyber attacks due to few if any cyber interconnections, there may be no cyber attack that would warrant a nuclear response. It may be advisable for the US to consider NC2 systems (especially for the US NC3 thinline) that do not rely on connections to the cyber domain as much as possible, until situational awareness in the cyber domain and behavioral normals are better defined and accepted internationally (but most especially with China and Russia).

B. RECOMMENDED STRATEGIES TO IMPROVE DETERRENCE IN THE CYBER AND SPACE DOMAINS.

Behavior norms are less well defined in the Cyber domain than any other warfighting domain, and it seems that this situation will persist into the near future.

In warfighting domains where behavior norms are well defined, it is easier for nations to work together to maintain stability and prevent conflict. For example, the United Nations Convention on the Law of the Sea (UNCLOS) seeks to codify the acceptable ways that nations can behave in the maritime domain. (UN Division for Ocean Affairs and the Law of the Sea, 2022) The treaty is not perfect, but it provides a foundation for how nations should, and should not, act in the maritime domain. Agreements such as UNCLOS provide clarity and understanding. Agreements

allow the majority of nations who are party to the agreement to mount a united front against those who would break the rules of the agreement, which in turn provides deterrence from breaking the agreement by those who would otherwise break it. In this way, international agreements provide stability and help prevent war.

Another treaty that has provided stability and clarity is the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (a.k.a. The UN "Outer Space Treaty" of 1967). This treaty defined that actions in space that can be taken for granted today. For instance this treaty, signed and ratified before the US had landed men on the moon, stated that sovereignty claims cannot be made of other celestial bodies, that weapons of mass destruction cannot be used in space, that celestial bodies cannot be used for any military purpose, and that all nations are free to explore space. (United Nations Office for Outer Space Affairs, 2022)

However, the cyber warfighting domain is newer, and therefore the behavior norms are less defined. In recent years, many nations have sought to establish rules of acceptable behavior in cyberspace. While numerous states have endorsed various international documents that touch on the issue, and several bilateral and plurilateral agreements have been reached, a comprehensive, multilateral framework governing state conduct in cyberspace has yet to materialize. Some observers have expressed hope that such an agreement will materialize in the near future, while others are more skeptical, arguing that the very nature of cyberspace makes it difficult to reach consensus on what constitutes appropriate state behavior. It is clear that many states are interested in developing norms of behavior in cyberspace, and that this process is likely to continue in the coming decades. The question asking "what actions in cyberspace require and justify a military response, and which may cross the nuclear threshold?" would be far easier to answer if the behavior norms for cyberspace were more clearly defined in international law and multilateral agreements. The US should endeavor to lead the way in this area and create enforceable agreements governing state behavior in cyberspace.

The second line of effort the US should undertake does not require cooperation with other nations. The design of the US Nuclear Command, Control, and Communications System, which relay emergency action messages (EAMs) and other vital communications from national leadership to US nuclear forces, should be designed so that any action in the cyber domain cannot remove positive control of US nuclear weapons from the President. The NC3 system is divided into the "thickline" and "thinline." The thickline consists of day-to-day and crisis architecture, it is not

designed to operate in all environments such as a trans nuclear environment and post nuclear environment. The thinline is designed to operate in all environments, including nuclear conflict. (Claeys, 2020)

Whereever possible the US NC3 thinline should not be reliant on the Cyber domain. Somewhat analogous to US Ballistic Missiles which do not require GPS to accurate arrive on target (since GPS can be denied by a competent adversary), relying on the cyber domain for operations of the NC3 thinline would be equally unwise.

While this point may seem obvious, it is not always obvious how such a complex system could interact with the cyber domain often indirectly. For instance, US Advanced Extremely High Frequency (AEHF) satellites communication signals are highly protected against a large number of nuclear and nefarious effects, and they are used for thinline NC3 communications. However AEHF spacecraft are also used for non-nuclear missions, and support of these mission may (theoretically) require an interface that accesses IP based communications from the world wide web, there may theoretically exist novel ways for an adversary to access these spacecraft through this type of threat vector.

It should be noted that the author of this paper intentionally did not access any classified information about how AEHF is actually controlled or how firewalls are maintained between information that has been passed from the internet, and the Command and Control of the spacecraft, to guarantee that no classified information could be unintionally revealed.

Disaggregation of nuclear communication systems may help guarantee positive control of US nuclear weapons for two reasons. Any single system can be interrupted or fail, and there have been examples of this historically. For example, on Oct 23rd 2010, a launch control center at F. E. Warran AFB in Wyoming lost contact with one of it's three squadrons of fifty nuclear armed miniman III ICBMs. In the launch facility down or "LF Down" condition crews in the control center could not communicate with the missiles for nearly an hour. The condition began when one of five launch control center computers began communicating erratically, triggering cascading communication errors that led technicians to take all five computers off-line. The incident was considered unusual and serious enough the Joint Chiefs Chairman, the Defense Secretary and the President were all notified.

The cause of the problem was later found to be a circuit card in one of the computers that had been improperly installed during routine maintenance. The misaligned circuit card disrupted the expected timing of the computer's regular automated signals to the missiles. This triggered the

cascade of error messaging that jammed the whole network. In cyber terms, the system executed a directed denial-of-service (DDoS) attack upon itself.

Crews in the missile control centers could not immediately determine whether the LF Down condition might be the result of malicious intrusion into the system. As a precaution, Air Force security officers were sent to the missiles to ensure their security. (Church, 2010)

Thus, the incident revealed a little appreciated danger: a loss of positive control over nuclear forces naturally raises concern that control has been blocked, or even usurped, by some malicious actor. That concern can influence decision-making even if the issue is an innocent glitch.

Disaggregation of communications routes for EAMs and other messages to reach their intended recipient, therefore, helps in two ways, it may help guarantee positive control is maintained, and it may help clarify whether an attack is underway vs something else such as a malfunction.

A networked NC3 system where multiple EAM routes exist that pass over many differing mediums would naturally be more difficult for an adversary to block all possible transmission routes. The number of possible transmission paths that exist in a networked system increases exponentially as the number of nodes increases. Resilience is also a benefit of a highly disaggregated networked system. Networks, if properly designed, can continue to accomplish their mission even when many of the communication nodes cease functioning. This provides natural protection against malfunction of any single or group of nodes, but it may also provide clarity as to whether a malfunction vs an attack is underway. Since any attack that is substantial enough to cause a failure of nearly all nodes in a large network would necessarily be large, it would also become clear to the victim that an attack was underway. Attributing a large attack is significantly easier than a minor attack since there would be far more attack vectors leaving clues as to which nation or organization is responsible. Therefore, a large network can provide robust and redundant communications paths that can only be disrupted adequately by a large attack that is more easily attributable.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SUMMARY

A. CONCLUSIONS

International law, policies, and established norms in other domains such as sea, land, and air add stability, and understanding, and provide clarity to potential adversaries' intentions in those domains, which reduces the likelihood of armed conflict due to misunderstanding or miscalculation. However, in the space and especially the cyber domains, international law, policies, and norms are not well established, which leads to destabilizing effects from misunderstanding of adversaries intentions, and miscalculations. Additionally, potential adversaries may view agreements as unenforceable if they do not believe that their actions can be observed or attributed to them, and may may lead them to take escalatory actions that they wouldn't dare take otherwise.

Usually, actions in the cyber and space domains by an aggressor intending to gain advantage over a victim must be done covertly. If the victim at any point becomes aware of the intrusion or vulnerability being exploited, the victim can usually protect itself by patching the vulnerability with more ease than it took for the aggressor to gain access, and the aggressor will have lost the advantage it once enjoyed.

Unilaterally, or with NATO and other allies, the US should endeavor to add systems that will provide situational awareness and visibility in these novel domains, to reduce the temptation by potential adversaries to take actions that they would not take if they knew their actions could be observed and attributed to them. US Cyber Command should make situational awareness in the cyber domain a top priority, while the US Space Command should do the same in the space domain. Adding situational awareness will take years and decades but should provide additional stability and transparency as it is achieved.

The US State Department, with specific recommendations from the Department of Defense (US Cyber Command, US Space Command, US Strategic Command, and other appropriate entities), should peruse international agreements to define norms in the space and cyber domains conducted by national militaries, especially actions that could undermine nuclear deterrence, the credibility of nuclear systems, and any systems used for Nuclear Command and Control (NC2).

Establishing nuclear redlines in the cyber domain without adequate situational awareness may not be as effective as in other domains. The relevant uniformed services (US Space Force, US Air Force, and US Navy) should, under the guidance of the proper combatant commands (US

Cyber Command, US Space Command and US Strategic Command), endeavor to reduce or eliminate NC2 cyber domain dependencies from the NC3 thinline. The goal would be to reduce, to the maximum extent possible, threats from the cyber domain on US nuclear systems, and nuclear credibility.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

The US Cyber Command should lead the research effort and investigate tools and strategies to gain additional situational awareness in the cyber domain. This should be an ongoing long-term effort requiring highly skilled cyber experts with precise knowledge of US classified systems in the DoD and elsewhere. The long-term goal is to gain enough situational awareness of US Government-owned systems such that potential adversaries cannot operate in the cyber domain with impunity, but rather must assume that their actions can be observed if their actions touch US DoD or US Government systems, especially those of US Nuclear Command and Control (NC2). The architectural changes needed to implement such situational awareness may be vast and require decades of updates to US Government systems. These changes should not unlawfully or unnecessarily encroach on US citizens' privacy, but rather apply to US Government systems only. However, recommendations and requirements could be provided to US companies and US DoD contractors to help protect against state-sponsored corporate espionage.

Similar to the recommendations for US Cyber Command above, the US Space Command should lead the effort to research and investigate tools and strategies to gain additional situational awareness in the space domain, as well as techniques for space control. This should be an ongoing long-term effort requiring highly skilled space systems experts with an awareness of specific US capabilities.

The US Strategic Command should lead the research effort into disaggregated mesh networked NC3 thinline architectures. In theory a mesh network could continue to operate even if multiple nodes were disrupted or destroyed. A network with a much larger variety of links between nodes may be more robust, provide more redundancy, and may make it more difficult for an adversary to disruptwithout revealing their identity.

Since geostationary spacecraft are few in number, and no longer safe from kinetic attack, it may be worth a shift in US NC3 thinline space architecture to a highly proliferated low earth orbit satellite constellation. Such a system may be more redundant, resilient, and more difficult to disrupt, and such a constellation would not necessarily cost more than a highly protected

geostationary constellation, since each spacecraft would be smaller, less expensive, and many could be placed in orbit per space launch. Many commercial companies have already pioneered the development of technology needed to facilitate such systems, and this technology could be leveraged.

THIS PAGE INTENTIONALLY LEFT BLANK

V. LIST OF REFERENCES

Brecher, M., Wilkenfeld, L., Beardsley, K., James, P., & Quinn, D. (2021). International Crisis Behavior Data Codebook, Version 14. Duke University.

Center for Strategic & International Studies. (2022, May). *Significant Cyber Incidents*. Retrieved from Center for Strategic & International Studies: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Church, A. (2010). Glitch Silences Minuteman ICBMs. *Air Force World*, 12.

Claeys, S. (2020, July 9). *NC3: Challenges Facing the Future System*. Retrieved from Center for Strategic & International Studies: NC3: Challenges Facing the Future System

Defense, U. S. (2020). *Defense Space Strategy.* Washington D.C.: United States Department of Defense.

George, J. P. (2019, March 27). *History of anti-satellite weapons: US tested 1st ASAT missile 60 years ago*. Retrieved from The Week Magazine: https://www.theweek.in/news/sci-tech/2019/03/27/history-anti-satellite-weapon-us-asat-missile.html

Gray, C. (2010). *The Strategy Bridge: Theory for Practice.* Oxford: Oxford University Press.

Harris, A. (2014, December 12). *Experts Skeptical North Korea Hacked Sony*. Retrieved from Fast Company: https://www.fastcompany.com/3040281/experts-skeptical-that-north-korea-hacked-sony

Jaikaran, C. (2021). *Federal Cybersecurity: Background and Issues for Congress.* Washington DC: Congressional Research Service.

La Trobe University. (2022, Sep 22). *La Trobe University Nest*. Retrieved from The fascinating evolution of cybersecurity: https://www.latrobe.edu.au/nest/fascinating-evolution-cybersecurity/

NASA Jet Propulsion Laboratory. (2022, September 22). *Explorer 1*. Retrieved from Jet Propulsion Laboratory: https://www.jpl.nasa.gov/missions/explorer-1

Office of the Director of National Intelligence. (2021). *Annual Threat Assessment.* Washington D.C.: Office of the Director of National Intellgence.

O'Neill, J. (2021, December 1). *Spae Force general says US satellites are attacked on daily basis*. Retrieved from New York Post: https://nypost.com/2021/12/01/space-force-gen-david-thompson-says-us-satellites-are-attacked-on-daily-basis/

Steinberg, M. (2021, Apr 14). *Bernie Madoff, mastermind of the nation's biggest investment fraud, dies at 82*. Retrieved from CNBC: https://www.cnbc.com/2021/04/14/bernie-madoff-dies-mastermind-of-the-nations-biggest-investment-fraud-was-82.html

UN Division for Ocean Affairs and the Law of the Sea. (2022, 07 13). *Oceans & Law of the Seas*. Retrieved from United Nations Webpage: https://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm

Union of Concerned Scientists. (2022, May 1). *UCS Satellite Database*. Retrieved from Union of Concerned Scientists: https://www.ucsusa.org/resources/satellite-database

United Nations Office for Outer Space Affairs. (2022). *Resolution adoped by the General Assembly*. Retrieved from United Nations Webpage: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html

United States Space Force. (2022). *United States Space Force Capabilities*. Retrieved from spaceforce.mil: https://www.spaceforce.mil/About-Us/About-Space-Force/Space-Capabilities/

US Department of Defense. (2020). *Defense Space Strategy.* Washington D.C. : US Department of Defense.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

THE RED LINE: NUCLEAR DETERRENCE IN THE DOMAINS OF SPACE AND CYBERSPACE

Kyle P. Santarelli SS3740 Spring 2022

The explosive destruction of Hiroshima and Nagasaki in 1945 marked the true beginning of the nuclear age. Since that fateful day, nuclear weapons have entered the arsenals of at least ten nations. Despite intense conventional conflicts and the obvious destructive effectiveness of nuclear arms, no nation has employed these weapons since their first use in World War II. Some may argue that simple rationality amongst world leaders has held this arrow in the quiver, however the truth about nuclear weapons use is much more complex. Strategic nuclear weapons, and in some ways tactical nuclear weapons, hold a critical role in the defense of a nation. The most effective deterrence against offensive use of nuclear arms is the threat of a devastating nuclear response. This nuclear deterrence provides security both from an adversary's nuclear arsenal as well as overwhelming destruction via air, land, and sea. (National Research Council et al. 2010) Equally as important as the maritime, land, and air domains, this paper explores the effectiveness of nuclear and non-nuclear deterrence in the age of Space and Cyberspace. This paper also proposes strategies to manage future escalation and improve deterrence across all warfighting domains. Nuclear and non-nuclear deterrence must adapt to meet the shifting warfighting paradigms. The United States must manage deterrence and contain the escalation of conflict in the Space and Cyberspace domains in order to ensure continuity of capability for warfighting forces.

Nuclear Deterrence

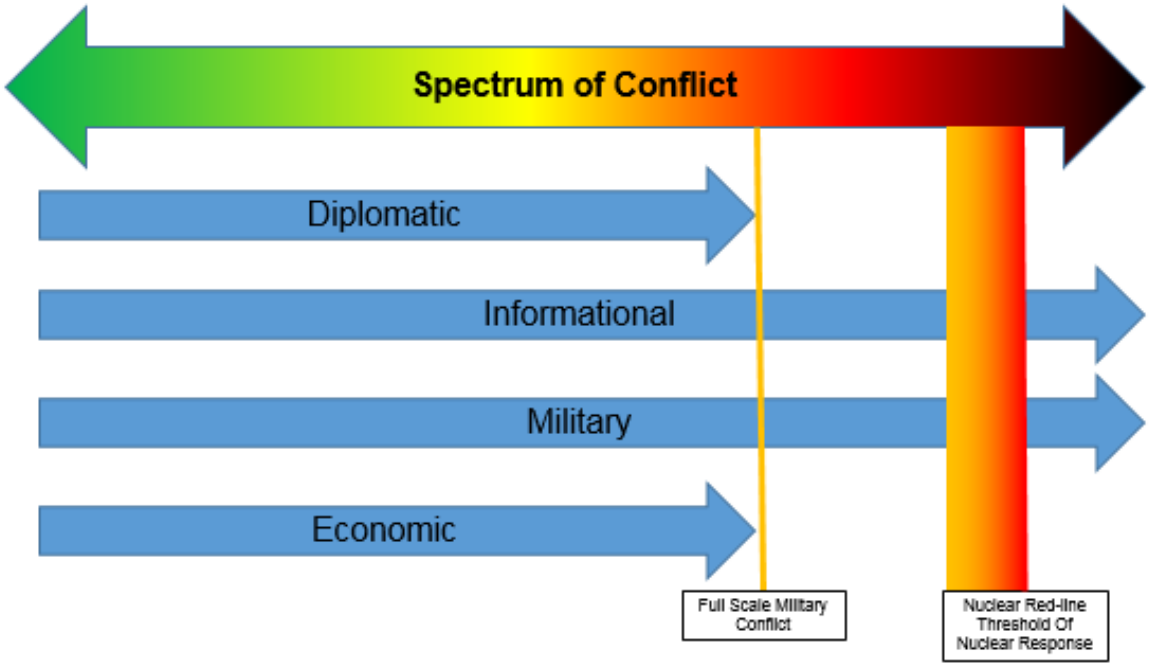
The standing policy of the United States leverages possession of nuclear weapons to achieve a tailored and flexible approach to impose unacceptable risks and intolerable costs for any potential adversary seeking egregious harm upon the United States.(US Government 2018) In this vein, nuclear capabilities are designed to deter nuclear attack as well as non-nuclear aggression. The threshold for American use of nuclear weapons is, and must remain, as high as possible. Despite this extremely high nuclear threshold, the policy of the United States does consider some types of adversary non-nuclear attacks as potentially exceeding this requirement, enabling response with nuclear means. One such example of a non-nuclear attack could be the employment of chemical or biological warfare against American citizens or territory. By including nuclear weapons in the available response options to such an attack, the adversary must consider the risks of a nuclear response. The calculus of such an attack is therefore heavily weighted by the potential for catastrophic imposed costs for crossing such a red line. This weighing of consequences by an adversary is the core element of nuclear deterrence. The nuclear arsenal is intended to "forestall war by showing a readiness to fight," rather than simply intended to

annihilate an adversary who oversteps in warfare.(A. B. Carter, Steinbruner, and Zraket 1987) Therefore effective deterrence must extend to all warfighting domains.

Deterrence of Non-Nuclear Attacks in Space and Cyberspace

Deterrence by Punishment

In an effort to forestall war, the United States must consider adversary aggression in space and cyberspace. Deterrence may be achieved through the threat of retaliation, known as deterrence by punishment. (M. Ruhle 2015) While the nuclear triad represents a credible capability to inflict catastrophic cost upon an enemy, other means of punishment must be considered below the nuclear threshold. The United States possesses a potential spectrum of responses to adversary aggression in Space and Cyberspace. Response options include the full range of available activities in the elements of national power: Diplomatic, Informational, Military and Economic (DIME). While some responses may be rather benign in nature, such as a political demarche or economic sanctions, this spectrum extends all the way to major conventional military action. Somewhere along this spectrum is where the nuclear red-line must be placed.



The nuclear threshold cannot be a clearly defined and communicated line, as publishing this information allows an adversary to effectively operate just short of this threshold. While some activities can be clearly communicated as over the line, such as nuclear strike, others may not be so clear cut. Actions in Space and Cyberspace inherently fall into this grey zone.

Deterrence by punishment in the Space and Cyberspace domains requires imposition of cost upon an adversary. The imposed costs must align with the scale of transgression, which may be difficult to quantify in these domains. A mirrored approach to certain activities at the peaceful end of the spectrum of conflict may be considered. Disruption attacks against the link segment of the space domain may be met with disruption attacks in kind. Jamming of non-critical communications links may also be met with imposed costs within another element of national power such as economic sanctions or diplomatic activity. In the Cyberspace domain, the scale of imposed cost requires examination of the scale of attack. Harassment of private sector entities in Cyberspace lies lower in the spectrum of conflict than Cyberspace attacks against Government infrastructure. Regardless, the Cyberspace activity must be examined in context of all actions taken by an adversary. The United States may seek to impose larger costs if Space and Cyberspace activities align with further escalation of a conflict or are designed to degrade the ability to command and control nuclear weapons.

Just like any domain, effective deterrence by punishment must meet three criteria: certainty, celerity, and severity. (D. Carter 2019) Certainty requires an adversary to understand that any action will be met with an imposed cost. Celerity requires the imposed cost to be swiftly applied so that any adversary action may be directly connected to the initial action. Severity of response must be in proper scale with the adversary action. Because of the lack of geographic association with the Space and Cyberspace domains, a swift and severe response may be imposed in any domain or with any element of national power, so long as a connection to the original adversary activity can clearly be ascertained.

Deterrence by Denial

As an alternative to, or in conjunction with, deterrence by punishment, the United States can also achieve deterrence by preventing an adversary from achieving their desired war aims. This prevention of an adversary's goals is known as deterrence by denial. Ideally, this is accomplished through defensive measures, known as *protection,* as well as ensuring continuity of the credible retaliation, known as *resilience*. (National Research Council 2010) More importantly, the United States must demonstrate a readiness to fight when aggression in these domains crosses an elevated threshold of damage to the American people. In sum, deterrence by denial is the amalgam of defense measures and measures of continuity. In the Space and Cyberspace domains protection and resilience must extend to all critical elements and mission areas. By limiting the damage an adversary may accomplish through offensive means, the likelihood of attacks in these domains may be diminished.

The space warfighting domain is not new or novel and has truly been a part of the calculus of deterrence since the launch of Sputnik on a Soviet R7 ICBM in 1957. For the Space domain, key mission

areas must fall under this umbrella of deterrence by denial. Missile Warning architecture in space, known as Overhead Persistent Infrared (OPIR) allows the United States to detect adversary strategic missile launches, a key element in nuclear warning. The GPS constellation both provides Position, Navigation, and Timing (PNT) as well as other critical missions for the DOD. Nuclear Command and Control communications links also operate on geostationary communications satellites. While protection of these assets may be difficult due to their placement in orbit, resilience may be accomplished through future disaggregation of systems into a multitude of smaller assets. Further resilience may be accomplished through redundancy across commercial satellite assets in a multitude of orbits. These missions are critically important to the continued operation of the DOD conventional and nuclear arsenals.

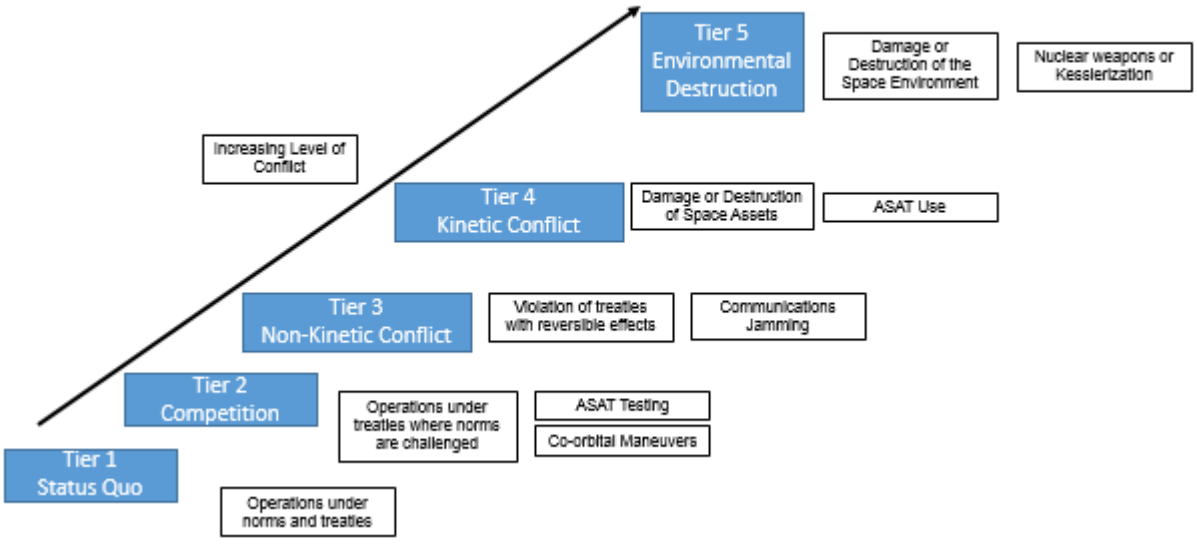
The Cyberspace domain stretches across national borders to encompass the international communications architecture as well as data transfer and storage of world community. Cyberspace also includes national SIPR and intelligence networks. Because of the important connections, information, and communications passing through cyberspace, protection and resilience in this domain is critical. Beyond DOD uses of cyberspace, the international economy relies upon uninterrupted operation of Cyber networks. Networks are also critical for economic, industrial, financial, and healthcare interests. Protection of Cyber networks requires defensive measures by individual operators, patching and maintenance of equipment. Resilience requires developing, coordinating, and hardening of redundant connections for critical links between systems. All of these activities must occur to develop and implement a deterrence by denial in Cyberspace. Deterrence is only once side of the nuclear puzzle, potential employment of nuclear arms must also consider the circumstances of conflict. Therefore it is prudent to examine escalation of conflict which could lead to the brink of nuclear war.

Escalation Management

When discussing escalation management, it is critical to distinguish between two different perceptions of the term “escalation”. This paper focuses solely on conflict escalation, the tit-for-tat increase in tensions, postures, activities, and warfare across the spectrum of conflict. Nuclear escalation, most often referred to as “limited nuclear escalation”, is not the intended focus of this paper. Current United States nuclear posture makes clear that flexible response options, including low-yield usage of nuclear weapons may be a component of deterrence. However, this is not designed to enable “nuclear war-fighting.”(US Government 2018) Escalation management is designed to reduce the likelihood that a conflict will cross the nuclear threshold, and this paper is not designed to provide recommendations once the threshold has been crossed.

Conflict Escalation in the Space Domain

Escalation management is inherently an effort to conduct conflict management scoped to a developing international situation between two or more countries. This management seeks to reduce, limit, or eliminate the level, scope, and intensity of violence in a conflict. (M. Melin 2015) There are a few tiers of conflict escalation in the space domain. These tiers represent levels of conflict which, once crossed, are incredibly difficult to back down from. Tier one is the status quo, governed by existing treaty and precedent, where nations act according to self-interest within existing norms. All conflict in the space domain exists as an escalation above this tier. The next tier is competition, wherein nations act in a manner within existing treaties, but not necessarily within existing norms, in an effort to gain a position of relative advantage in space. Tier three is non-kinetic conflict, in this tier actions and activities are undertaken to inhibit, interfere, or disrupt activities of another nation. This tier is the first in which international agreements on non-interference are violated. Tier four is kinetic conflict, where on-orbit assets are permanently damaged or degraded by activities undertaken to gain an advantage in a conflict. Tier five includes potential crossing of the nuclear threshold and includes attempted destruction of the operating environment for spacecraft in a specific orbital regime.



Due to reliance on space assets for modern warfighting, it is imperative to manage future conflicts in space at or below Tier 3. Non-kinetic conflict allows for the continued survival of space based assets to support the warfighter. Efforts must be undertaken to ensure that the United States does not escalate the conflict to Tier 4. To accomplish this escalation management, the United States should exercise all elements of national power to impose costs between the transitions from Tier 2 to Tier 3. Deterrence by punishment in this transition should be coupled with clear diplomatic communication of the consequences

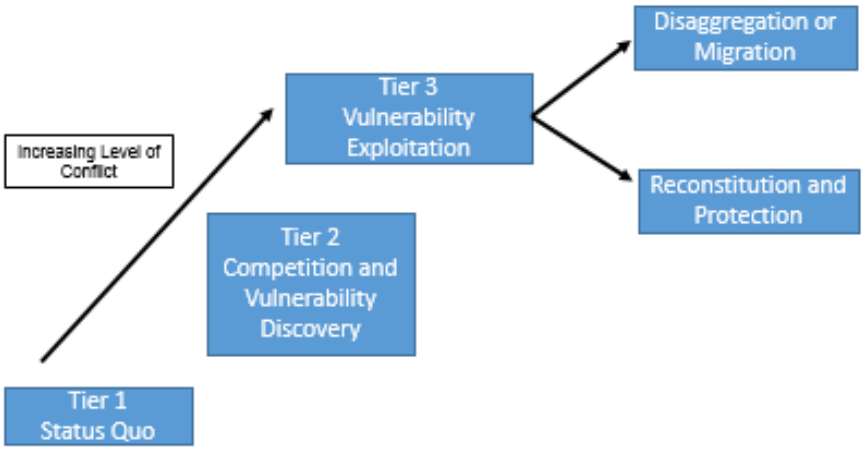
if the adversary wishes to transition to Tier 4. The adversary should not believe that they can move into kinetic destruction of U.S. space assets without an overwhelming burden of imposed costs. Furthermore, imposed costs should be heavily weighted in alternate domains such as air, maritime, or sea, as to not unintentionally further escalate the situation in the space domain.

At every stage of a conflict, the United States should offer potential off-ramps for the adversary. In no way should the United States only offer an adversary the only choice but to escalate a conflict. Available off-ramps in the space domain may include diplomatic communication, quid pro quo force withdrawal, and tactical pauses in escalatory measures. If the threshold into kinetic conflict is crossed, the U.S. should make every effort to limit the continuation of conflict in the space domain. This does not mean that the U.S. should halt all activity, but rather continue operations in tier 3 without significant escalation of U.S. activities into the Space kinetic tier of conflict. Should escalation in this domain spiral out of control, only then should the U.S. respond above tier 3. Kinetic destruction of non-critical space assets, or even partial destruction of the AEHF constellation may rise to the nuclear threshold, but these activities must be placed in the context of the greater conflict. Decisions on activities in space should be made with the greater understanding of continuation of critical capabilities for other domains.

Conflict Escalation in the Cyberspace Domain

In a similar manner to the Space domain, escalation in the Cyberspace domain must be managed to preserve capabilities for the United States and the warfighter in a potential conflict. However the tiers of conflict in Cyberspace differ significantly from the linear escalation of the Space domain. Tier 1 is status quo operations in the cyberspace domain wherein all members of the international community leverage the domain for economic, industrial, or financial purposes. This tier is governed by the norms and standards of the open internet. In this tier, individual members build deterrence by denial through building of protection and encryption into their networks. In this tier, adversaries posture themselves for defense, but retain the capability to cause damage to potential adversaries. As conflict escalates, adversaries operate in a competitive manner. This second tier of conflict incorporates exploration of vulnerabilities in cyberspace. These vulnerabilities may be present in national systems, but are also in economic systems, such as defense contractors, banking networks, or healthcare networks. Unlike the space domain, where the primary target is military capabilities and communications, the cyber domain extends to include many civilian and commercial targets. The next tier of conflict includes the exploitation of these vulnerabilities. In this tier, actions in Cyberspace are undertaken to “disrupt, confuse, demoralize, distract, and ultimately diminish the capability of the other side.” (Cimbala 2017) Unlike the space domain however, this escalation cannot continue to higher threat levels. As a vulnerability is exploited, the

targeted system is either protected, modified and constituted, or migrated to different systems across cyber space.



Management of escalation in Cyberspace stems from choices made based upon discovered vulnerabilities. The United States must choose which discovered vulnerabilities should be pursued. The effects of an exploited vulnerability must be considered in the context of a conflict. A vulnerability in an industrial target may be less escalatory than exploitation of a vulnerability in an adversary's national communication. Furthermore, the United States should implement deterrence by denial by expending every effort to protect the most critical capabilities, preventing the adversary from inflicting significant harm upon U.S. warfighting capability. The United States can also reserve the most severe discovered vulnerabilities to respond through deterrence by punishment for adversary actions in cyberspace. The nuclear threshold in Cyberspace is difficult to define, as effects of an adversary's cyber-attacks may be unintended. A nuclear threshold can only be examined in the context of a greater conflict, should alternate domain attacks coincide with a cyber-attack on nuclear architecture, and this may rise to meet the nation's nuclear threshold. An isolated network attack which has impacts on nuclear command and control may not meet the threshold so long as a significant measure of nuclear continuity remains. Intelligent leadership must assess the impacts of any attack, and consider retaliation options up to and including nuclear weapons use. Ultimately, the activities in cyberspace must be undertaken to support other domains and prevent the further escalation of a conflict to near the nuclear threshold.

Conclusion

Nuclear and non-nuclear deterrence in the Space and Cyberspace domains requires significant planning, coordination, and execution. The goal of preventing or mitigating attacks against the United States needs a comprehensive spectrum of options to manage the escalation of a conflict. Deterrence relies upon the two-pronged effort of deterrence by punishment and deterrence by denial. Deterrence by punishment leverages the imposition of costs across all elements of national power. This deterrence is critically important in the space domain, imposing costs in other domains to prevent irreversible damage to the Space capabilities on which the warfighter relies. Deterrence by punishment in the cyber domain requires the discovery and careful execution of exploitation. Deterrence by denial in the space domain requires future disaggregation and redundancy of critical space capabilities. Managing the escalation of a conflict in space is also critical to the continuation of nationally important capabilities. Network protection remains a cornerstone of deterrence by denial for the cyber domain. Reconstitution of disrupted or damaged networks serves to ensure the continuity of operations, and must also be prioritized. Escalation management in the cyber domain may require restraint in the choice of vulnerability exploitation. Ultimately, the United States must manage deterrence and contain the escalation of conflict in the Space and Cyberspace domains in order to ensure continuity of capability for warfighting forces.

Sources:

Carter, Ashton B., John D. Steinbruner, and Charles A. Zraket. 1987. *Managing Nuclear Operations*. 1st ed. Washington, D.C., UNITED STATES: The Brookings Institution.

Carter, David. 2019. "8.3. Deterrence." https://openoregon.pressbooks.pub/ccj230/chapter/8-3-deterrence/.

Cimbala, Stephen J. 2017. "Nuclear Deterrence and Cyber Warfare: Coexistence or Competition?" *Defense & Security Analysis* 33 (3): 193–208. https://doi.org/10.1080/14751798.2017.1351142.

Melin, Molly M. 2015. "Escalation in International Conflict Management: A Foreign Policy Perspective." *Conflict Management and Peace Science* 32 (1): 28–49.

National Research Council, Policy and Global Affairs, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, and Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. 2010. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U. S. Policy*. Washington, D.C., UNITED STATES: National Academies Press. http://ebookcentral.proquest.com/lib/ebook-nps/detail.action?docID=3378670.

"NATO Review - Deterrence: What It Can (and Cannot) Do." 2015. NATO Review. April 20, 2015. https://www.nato.int/docu/review/articles/2015/04/20/deterrence-what-it-can-and-cannot-do/index.html.

US Government. 2018. "Nuclear Posture Review." USG.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

Cross-Domain Dynamics and the Effect on Aggression, Escalation, and Deterrence in a Nuclear Environment

LT LEVI ROSA

March 2022

The United States' National Defense Strategy states, "The Department of Defense's enduring mission is to provide combat-credible military forces needed to deter war and protect the security of our nation. Should deterrence fail, the Joint Force is prepared to win.(Mattis)" Deterrence, however, has rapidly evolved over the last decade with advances in the space and cyber domain. These domains are becoming progressively more interconnected in both conventional and theoretical nuclear conflicts, disrupting traditional strategies involving aggression, escalation, and deterrence. Due to the infancy of these domains, behavioral norms have yet to be established and with many assets that are dual tasked with conventional and strategic missions, interactions within these domains are not transparent or predictable. The focus of this paper is to determine how these cross-domain dynamics affect existing deterrence posture and escalation management strategy. The paper will focus on three main questions; How can aggression be measured across domains that influence nuclear deterrence and escalation management, what strategies exist to manage escalation and improve deterrence, and what is the nuclear threshold in the space and cyber domains?

"Aggression, in international relations, is an act or policy of expansion carried out by one state at the expense of another by means of an unprovoked military attack (Britannica). "While this definition of aggression is straight forward, it fails to acknowledge that aggression can appear in many forms. Aggression can be exhibited though the instruments of national power, diplomatic power, information power, military power, and economic power (DIME). This brings us to our first questions; how can aggression be measured across domains that influence nuclear deterrence and escalation management?

Let us look at military power and the tools our adversaries have in the space and cyber domains to help us understand how aggression can be measured and how we can manage escalation. In the Defense Against the Dark Arts in Space, Todd Harrison, Kaitlyn Johnson, and Makena Young discuss five categories of counterspace weapons; kinetic physical, non-kinetic physical, electronic, and cyber (Harrison et al.). Along with these weapons come two categories of the effects they could impose on our space assets: reversible and non-reversible. Reversible being

effects that are temporary and would impose low consequences because they have a low potential to cause major damage in space. Where non-reversible effects would be permanent and would impose high consequences because they would render our space asset attacked inoperable. This leads to the counterspace continuum pictured below in Figure 1 which illustrates these types of counterspace weapons from reversible to non-reversible.

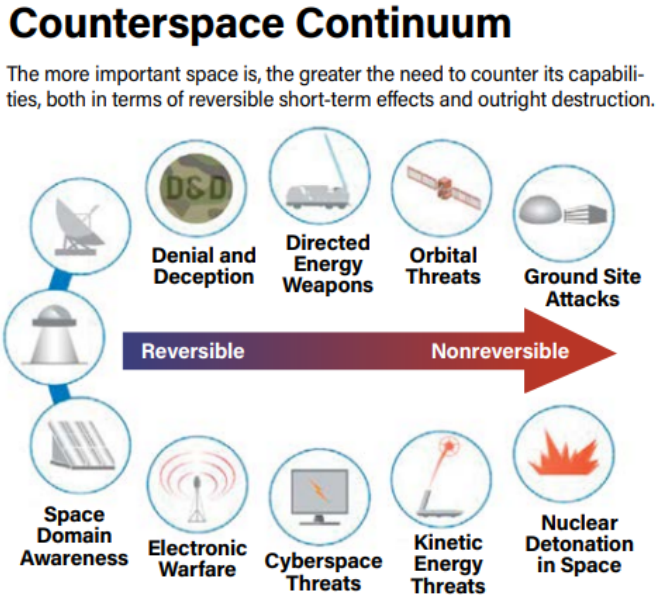


Figure 2: Counterspace Continuum ("Counterspace Continuum")

The implementation of any counterspace weapon can be seen as an act of aggression, but due to the nature of its effects will constrain the United States' response. Other factors that must not be ignored are the assets being targeted by these counterspace weapons (are they vital to national interests), what is the current political environment with our adversaries, and what is the frequency of attacks. The situation quickly gets more complex when more factors are added to the scenario. Is the space asset being targeted used for conventional or strategic missions or perhaps it's a dual use system? Are we currently engaged in other aspects of aggression with our adversary within the DIME construct? In terms of how aggression is measured across domains that influence nuclear deterrence, it can directly fall in line with the counterspace continuum. Reversible effects like space domain awareness, electronic warfare, cyber attacks will be measured as levels of low aggression. Non-reversible effects like orbital strikes, ground site attacks, and nuclear detonations in space will be measured as high levels of aggression. The frequency of attacks will affect the level of aggression and will increase with more attacks. The same relationship can also be seen

with higher value assets that have more strategic importance. This relationship can be seen in figure 2 below.

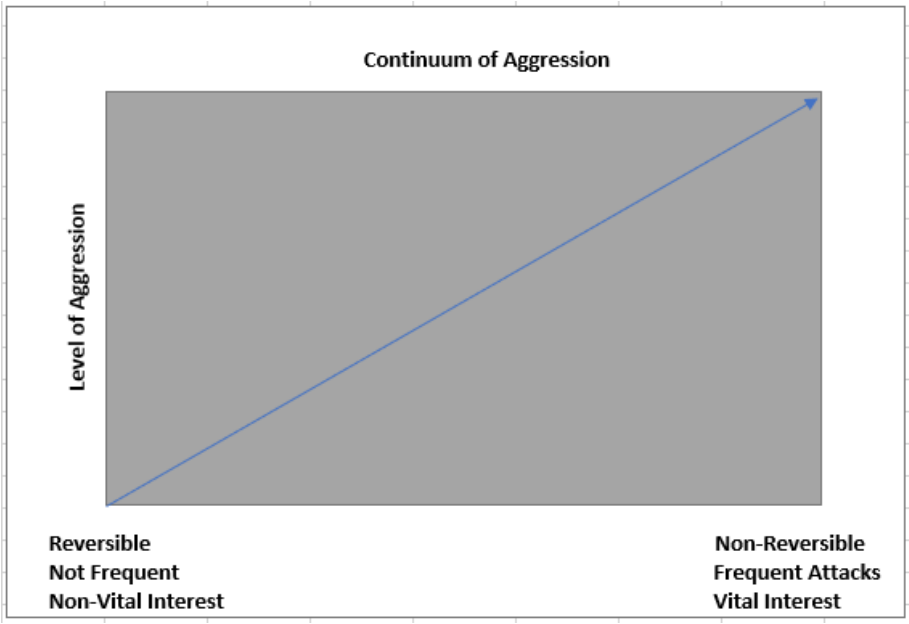


Figure 3: Continuum of Aggression

Figure 2 shows a simple linear relationship, however in reality when you start to mix the variables on the x-axis into one scenario it makes things a lot more complicated. For example, if an attack that has reversible affects is conducted on a strategic space asset that provides critical capabilities to the nuclear triad this may show high levels of aggression. This scenario contradicts figure 2 because it shows reversible affects all the way on the left with low levels of aggression and vital interest all the way on the right with high levels of aggression. This just shows the complex nature of the problem. There isn't an exact method to measure aggression. All factors must be considered, from what weapon is being employed, what is being attacked, how many assets are being attack and how frequent, how important is this asset to national security, and what is the current political environment.

There are numerous ways to manage escalation and improve deterrence. To do this we must first understand the strategies that are available to us. In a paper titled New Challenges in Cross-Domain Deterrence, King Mallory suggest three broad categories for deterrence strategies: non-escalatory to escalatory approaches, reversible to irreversible measures, and denial to punishment (Mallory). Each of these categories encompass two ends of the spectrum of action like that of the counterspace continuum discussed earlier. Figure 3 displays these categories into eight distinct

levels of strategies that can be utilized in deterrence. In ranking order from least to most severe in action, these deterrence strategies are:

1. Non-escalatory Reversible (Denial)
2. Non-escalatory Reversible (Punishment)
3. Non-escalatory Non-Reversible (Denial)
4. Non-escalatory Non-Reversible (Punishment)
5. Escalatory Reversible (Denial)
6. Escalatory Reversible (Punishment)
7. Escalatory Non-Reversible (Denial)
8. Escalatory Non-Reversible (Punishment)

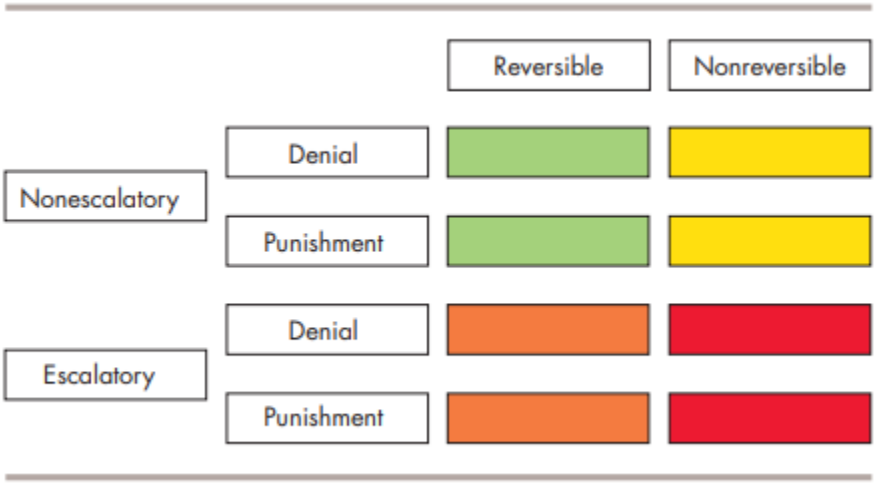


Figure 4: Deterrence Strategies (Mallory)

At one end of the spectrum, you have the reversible non escalatory denial strategy. This strategy seeks to respond to the adversary without escalating the situation while implementing reversible countermeasures without punishment. This is the ideal situation because deterrence is costly and the ability to de-escalate a conflict deliberately is important to successful crisis management (Mallory). At the other end of the spectrum is the opposite scenario of an escalatory nonreversible punishment strategy. This strategy seeks to deter our adversaries by escalating the situation with nonreversible effects that inflict high costs on the adversary. This method is not preferred because it can lead to more conflict, costs, and loss of life. To manage escalation the United States must utilize the correct deterrence strategy for the given situation.

How do cross domain dynamics affect these escalation management strategies? To understand these dynamics, we must first understand what cross domain means. Vincent Manzo at The Institute for National Strategic Studies provides us with two definitions of cross domain. Cross-domain could be defined according to the platform from which an actor launches an attack and the platform on which the target resides (Manzo). With this definition of cross-domain an attack from an aircraft to a naval vessel would essentially be a cross-domain attack. With the addition of space and cyberspace into the available operational domains this definition just enables more options to the United States and adversaries in their escalation management calculus. With five domains there are twenty cross-domain interactions possible from one domain to another if we are only considering two domain interactions (Figure 4).

Space-Cyber	Cyber-Space	Land-Space	Air-Space	Sea-Space
Space-Land	Cyber-Land	Land-Cyber	Air-Cyber	Sea-Cyber
Space-Air	Cyber-Air	Land-Air	Air-Land	Sea-Land
Space-Sea	Cyber-Sea	Land-Sea	Air-Sea	Sea-Air

Figure 5: Cross-Domain Interactions

Manzo's second definition of cross-domain refers to the effects of an operation. Under this method, an attack is cross-domain if its expected effects develop in a different domain than its target. (Manzo). It is with this definition where you can see the implications of cross-domain dynamics and how space and cyberspace are a real game changer. "For example, U.S. precision conventional strike operations depend on access to multiple domains. A potential adversary might be incapable of destroying U.S. aircraft or nuclear-powered cruise missile submarines, but it might be able to attack the space and cyber assets that enable these platforms to destroy targets. This appears to be the logic underlying China's interest in counterspace and cyber-attacks: such attacks shift the conflict to domains where China's offensive forces have an advantage over U.S. defenses, thereby altering U.S. capabilities in domains (air and sea, for example) where China would otherwise be at a disadvantage (Manzo)." So, while China may not have the advantage over our naval fleet, due to our reliance on the space and cyber domains, they can expose this and gain an advantage by targeting these domains for desired effects in the sea domain.

The big question is how do we improve deterrence with these cross-domain dynamics? The answer is quite simple, and it falls back to our National Security Strategy (NSS). The priority actions in the United States' NSS are modernization, acquisition, capacity, improve readiness, and

to retain a full-spectrum force (Trump, Donald). Modernizing our current weapon systems to include space and cyber assets will help in improving deterrence. This same theme is observed in the 2018 Nuclear Posture Review (NPR). The NPR emphasized that we must modernize our nuclear ballistic missile submarines, strategic bombers, nuclear air-launched cruise missiles, intercontinental ballistic missiles (ICBMs), and associated nuclear command and control (Mattis, Jim). In addition to this we must modernize our counterspace and cyberspace capabilities to that of the Chinese and Russians who are putting a lot of attention to these domains. If the perspective is that we have a modern capable capability in all domains than an adversary will think twice before acting.

New approaches to acquisitions will improve deterrence because it will allow us to field capabilities faster and more efficiently. The current bureaucracies involved in the acquisitions process frequently lead to over costs and delays in fielding new assets and capabilities. Without these bureaucracies we can be more innovative and seek other means of acquisition like relying more on the commercial sector to field new capabilities. This approach to acquisitions for space capabilities is even more important as we are going though essentially another space race. If we can put out new technologies on pace or faster than that of our adversaries than we will be able to become a harder target and actions taken against the United States would be less likely.

The NSS mentions capacity as one of the nations top priorities. It makes sense that a large military force would increase deterrence because you don't want to attack someone that has a larger military than you. While the NSS focuses on the size of our force there are more aspects of capacity that should be observed. Specifically, within the space domain we want to have large satellite constellations with redundancy and resilience. A proliferated space architecture has many advantages to improve deterrence. Multiple payloads that perform the same function on multiple satellites makes it harder for an adversary to eliminate those capabilities entirely thus deter actions in the space domain. Proliferated architectures are naturally resilient to jamming and can overcome challenges in the electromagnetic spectrum. With a proliferated architecture the United States can also reduce the number of dual use systems to understand adversary actions in space. Separating conventional and strategic mission payloads will be important to the United States responses to actions taken against them in space. The United States currently working towards this goal of a proliferated National Operational Architecture (NOA) though Project Overmatch. Overmatch ranks No. 2 on the Department of Defense's spending budget, which emphasizes its importance and it's a key contributor to the military's plans for joint all-domain command and control

(Tadjdeh). A resilient cross-domain capability in space will allow the United States to deter aggression within all operational domains.

Improved readiness is another key factor in increasing deterrence. Having a force deployed around the world ready to act at any moment has been a part of the United States' deterrence strategy from the beginning. This hasn't and will never change. The aspects that will change are the tools available to the warfighter and the domains which we are operating in. In the context of this paper the cross-domain dynamics for improved readiness rely with the warfighters ability to respond within the space and cyber domains. To maintain deterrence across all domains the United States must improve in space and cyber space readiness. These domains are untested in major conflict and because of their infancy there are a lot of unknowns. Warfighters need to be aware of what space or cyber assets they have available to them, and they need to know how to use them.

The last priority in the United States' NSS was to retain a full-spectrum force. What that means is what we have been talking about all along, to improve deterrence the United States needs to be able to operate in all domains simultaneously and be able to counter various types of threats. The NSS states, "The Department of Defense must develop new operational concepts and capabilities to win without assured dominance in air, maritime, land, space, and cyberspace domains, including against those operating below the level of conventional military conflict." While an advantage may not be had in all domains, by utilizing all-domain operations the United States will be more successful because it will be able to act with the cumulative information of multiple domains than that of a single domain. This type of posture sets the United States up as a hard target and improves deterrence.

The final focus of this paper is to understand what the nuclear threshold is in the space and cyber domains? The nuclear threshold is defined as a point in a conflict at which nuclear weapons are or would be brought into use (Oxford). The NPR states, "The United States would only consider the employment of nuclear weapons in extreme circumstances to defend the vital interests of the United States, its allies, and partners. Extreme circumstances could include significant non-nuclear strategic attacks. Significant non-nuclear strategic attacks include, but are not limited to, attacks on the U.S., allied, or partner civilian population or infrastructure, and attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities. The United States will not use or threaten to use nuclear weapons against non-nuclear weapons states that are party to the Non-Proliferation Treaty (NPT) and in compliance with their nuclear

non-proliferation obligations (Mattis, Jim)." The United States isn't likely to jump straight into a nuclear conflict. To reach the nuclear threshold a conflict would likely have already been going on for some time with some conventional kinetic exchanges. The point at which threshold would be achieved would be when an adversaries began to target population centers and capabilities which are a part of our nuclear response. Within the space and cyber domains, the following are the most likely reasons for crossing the nuclear threshold:

1. Nuclear Detonation in space
2. Kinetic or Non-Kinetic Anti-Satellite Attack on Nuclear Command, Control, and Communications (NC3) Space Architecture
3. Cyber-attack or kinetic attack on ballistic missile submarines, strategic bombers, nuclear air-launched cruise missiles, ICBMs, and associated nuclear command and control to include ground stations.
4. Massive cyber-attack on the United States infrastructure (power grid, economy, total disruption of day-to-day life)
5. Similar attacks of our allies.

This list of actions against the United States would be in a scenario in which ongoing escalatory actions have already been conducted. While the list above may not hit on everything, its important to note that this is a last resort in the scenario in which deterrence fails. The space and cyber domains don't really change the nuclear thresholds; however, they act as new mediums in which an adversary can use to get to that there. For that reason, it is important for the United States to keep its space and cyber capabilities modernized and on par with adversary capabilities.

In conclusion, the infancy of the space and cyber domains bring with them many challenges for the Untied States. The lack of experience and behavioral norms within these domains makes the decision-making calculus difficult not just for the United States, but its adversaries as well. The U.S. Government and potential adversaries lack a shared framework for analyzing how concepts such as proportionality, escalation, credibility, and deterrence apply when capabilities in space and cyberspace not only enable operations in other domains but also are part of the battlefield (Manzo). This paper sought to acknowledge three focus areas; How can aggression be measured across domains that influence nuclear deterrence and escalation management, what strategies exist to manage escalation and improve deterrence, and what is the nuclear threshold in the space and cyber domains? After analyzing the first two questions you quickly see that they are directly related to each other. Acts of aggression are directly linked to the types of capabilities employed by

a state actor; capabilities that deliver reversible and non-reversible effects. When looking at the strategies available by a state actor, it is also related to reversible and non-reversible effects. Its not in the United States' best interest to go into total war, which is why deterrence is our priority. To increase deterrence the United States must modernize its forces, streamline acquisitions, increase the size of its forces and assets, increase its warfighters level of readiness, and be prepared in all-domains to act. All of this is to avoid reaching the nuclear threshold. No nation wants to go there, but if they must protect their people and vital interest they will. While the space and cyberspace domains change a few things, the foundations of nuclear deterrence remain the same. Space and cyberspace are just new mediums for warfighters to navigate tough and another calculation in our decision-making calculus.

Sources:

Britannica. *Aggression*. 2021, https://www.britannica.com/topic/aggression.

"Counterspace Continuum." *Airforace Magazine*, 2021, https://www.airforcemag.com/app/uploads/2020/11/Counterspace_Continuum.pdf.

Harrison, Todd, et al. *Defense against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons*. Center for Strategic and International Studies (CSIS), 2021.

Mallory, King. *New Challenges in Cross-Domain Deterrence*. RAND Corporation, 2018. *DOI.org (Crossref)*, https://doi.org/10.7249/PE259.

Manzo, Vincent. *Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?* p. 8.

Mattis, Jim. *Nuclear Posture Review*. Office of the Secretary of Defense, Feb. 2018.

Mattis, Jim. "Summary of the 2018 National Defense Strategy." *Office of the Secretary of Defense*, 2018, p. 14.

Oxford. "Nuclear Threshold." *OxfordLanguages*, 2021, https://languages.oup.com/google-dictionary-en/.

Tadjdeh, Yasmin. *Navy Dedicates More Resources To Secretive Project Overmatch*. p. 7.

Trump, Donald. *National Security Strategy*. The White House, Dec. 2017.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C

Bryan P. Lay, Lieutenant Commander, U.S. Navy
SS3740: Nuclear Command, Control, and Communications – Part I
December 15, 2021

Introduction

Space and nuclear policy have an intertwined history with space as an enabler of nuclear operations, defense, and early warning. The release of the 2018 Nuclear Posture Review has awakened thought as to the relationship between cyber and nuclear operations, with the potential for cross domain deterrence and retaliation. The Nuclear Command, Control, and Communication system (NC3) reliance upon space and cyber enabled systems disrupts traditional strategies involving aggression, escalation, and deterrence. The cross-domain reliance of space, cyber, and nuclear systems result in the affirmation that affects in the cyber or space domains, under certain circumstances, warrant a nuclear response. To determine the threshold of these circumstances one must evaluate threat environment, determine adversary intent, and properly anticipate world perception of retaliatory actions.

Background

The United States remains committed to the vision of a world free of nuclear weapons but realizes their necessity to counter and deter global threats. Today the U.S. faces a more diverse and advanced nuclear threat environment with adversary development of new weapons and deployment systems.[1] To meet adversary development and deployment of tactical nuclear weapons, the NPR lays out a modernization plan which includes conversion of some SLBMs to low yield and development of new low-yield warheads. Critics' analysis of U.S. intent to develop new, low yield, tactical nuclear weapons assume a lower threshold for U.S. employment of nuclear

[1] NPR Executive Summary p.V

weapons. It is easy to assume a lower impact nuclear weapon may enter a leaders decision calculus earlier of more often, but that is not the intent of such weapons. U.S. nuclear policy remains on a posture of deterrence; with adversary nations developing and considering employment of tactical nuclear weapons, the U.S. must be able to meet in kind retaliation.

While the current NPR offers little departure from the Bush and Obama administrations, it does add key language addressing non-nuclear strategic threats and capabilities, mentioned 37 times, and cyber as one such non-nuclear strategic threat, 16 times.

> *"Effective U.S. deterrence of nuclear attack and non-nuclear strategic attack requires ensuring that potential adversaries do not miscalculate regarding the consequences of nuclear first use, either regionally or against the United States itself. They must understand that there are no possible benefits from non-nuclear aggression or limited nuclear escalation."*[2] *... "To correct any Russian misperceptions of advantage and credibly deter Russian nuclear or non-nuclear strategic attacks—which could now include attacks against U.S. NC3—the President must have a range of limited and graduated options, including a variety of delivery systems and explosive yields."*[3]

These statements portray a new environment in which nuclear warfare becomes increasingly possible by viewing non-nuclear strategic attacks, specifically cyber-attacks on the NC3 system, as sufficient justification for a nuclear response.

Aggression

Traditional force posturing and diplomatic signaling are difficult at best to fully understand and to carry out a de-escalation or deterrence is even more complicated. If it were simple, the Cold War may have been prevented or at least minimized. Exquisite national systems helped bring threat environment into focus and aided decision makers to bring Cold War hostilities from the complicated down to the complex problem domain, but the operational environment is now beyond what can be simply seen. Cyber and space domains share a common obscure nature in which they

[2] NPR Executive Summary p. VII
[3] NPR p 31

cannot easily be observed or verified as traditional domain forces. Action in space can be monitored to a degree with robust, yet limited, space domain awareness systems. Determination of intent and potential aggression is challenging as claims of non-operational or malfunctioning satellites could cloche adversary actions. With satellite motherships deploying addition child satellites and further limitations in cislunar domain awareness, ownership of a specific space asset, let alone attribution, are not always possible. The ambiguity of these domains makes it challenging to respond and decrease the likelihood of lowered nuclear threshold in response to such actions due to the lack of surety.

The Peoples Liberation Army's doctrine stresses space as vital to winning its future wars. "Chinese military strategists began writing about the targeting of space assets as a "tempting and most irresistible choice" in the late 1990s, and the People's Liberation Army has been pursuing the necessary capabilities ever since."[4] In addition to direct assent ASAT demonstrations, China has been observed conducting co-orbital maneuvers with a satellite capable of grappling another satellite with a robotic arm.[5] These action coupled with China's hypersonic fractional orbital delivery system test display a level of force posturing to act in both space and nuclear realms. Russia's demonstration of their "nesting doll" satellites conducting proximity operations with a known U.S. spy satellite[6] and their recent anti-satellite missile test prove their willingness to engage in the space domain.

Cyber attribution proves just as challenging with state and non-state actors working independently and co-operatively using node obscuring techniques and non-native tool sets in their engagements. During the height of the pandemic the general public received a preview of what

[4] Loverro, D. Statement of Douglass Loverro Deputy Assistant Secretary of Defense (Space Policy) before the Subcommittee on strategic forces house armed services committee, March 15 2016, 5
[5] Weeden, B. & Samson, V. Global Counterspace Capabilities: An Open Source Assessment, April 2020, Secure World Foundation, 1-4 – 1-5
[6] W. J. Hennigan, Time, February 10 2020, https://time.com/5779315/russian-spacecraft-spy-satellite-space-force/

effects cyber activity can have on critical infrastructure. The attacks on Dominion power, pipelines, and meat processing facilities exasperated supply chain issues and consumers were impacted at the grocery store and at the pump. These types of small scale cyber activity temporarily crippled regions and plant seeds of civil unrest. Considering the abilities and scale of attacks possible by a nation state, one must consider the overall economic, political, and civil consequences an adversary could impose by way of cyber alone.

For both space and cyber, on occasions where positive attribution is possible it may not always be advisable to disclose or react due to U.S. capabilities or partnerships being revealed which may cause greater implications to national defense. In those instances, a like kind and covert response is more appropriate. The effects of the attack will likely dictate the U.S. response, but thresholds are not formally established and ill perceived.

Thresholds

> *"There is no "one size fits all" for deterrence. Consequently, the United States will apply a tailored and flexible approach to effectively deter across a spectrum of adversaries, threats, and contexts. Tailored deterrence strategies communicate to different potential adversaries that their aggression would carry unacceptable risks and intolerable costs according to their particular calculations of risk and cost."*
> *- NPR VII-VIII*

At present, there is not a true deterrence in the cyber and space domains, only a promise of like kind retaliation. While mutually assured destruction may work as a deterrent for nuclear threats it has limited effect elsewhere. Computers and satellites can be reconstituted, orbital debris concerns will be shared by both foes, loss of life is unlikely, and the magnitude physical harm in minimal in comparison. For these reasons one cannot justify nuclear action in retaliation or as a deterrent broadly in the cyber and space domains. Loose vernacular in the 2018 NPR leaves an impression that a cyber attack could represent a nuclear threshold and is a hazardous policy shift with a potential to increase the risk of premature nuclear escalation. Former Secretary of Energy,

Ernest Moniz, concurs with this assessment in stating "the entire broadening of the landscape for nuclear deterrence is a very fundamental step in the wrong direction…I think the idea of nuclear deterrence of cyberattacks, broadly, certainly does not make any sense."[7] If the former U.S. secretary carries this impression one can only assume that a potential adversary sees it as well. Views as this could result in an adversary believing either U.S. deterrence is hollow or hostile. If the U.S. relays upon to heavily upon nuclear arms for cross domain deterrence our "threats come to be perceived as a general policy of hostility, they may lose their ability to be applied to deter specific actions."[8]

Deterrence is required to prevent or limit conflict, but it must come from other domains with a whole of government approach. "Of particular concern are expanding threats in space and cyber space, adversary strategies of limited nuclear escalation."[9] The United States has recently embarked on a mission to declassify multiple space sensor and warfare capabilities. Knowledge of capabilities brings credibility to deterrent threats by signaling to an adversary their actions are more likely to be attributed, thus reacted upon. If deterrence fails, "China's expanding non-nuclear military capabilities include space and cyber warfare capabilities could decisively affect the outcome of a conflict."[10] The specific conflict and likely outcome would have to be weighted to see if nuclear response may even be considered. Losing a conflict may be acceptable if U.S. sovereignty is not compromised. Furthermore, it may be preferable than conducting a nuclear first strike ushering in a new era of nuclear conflict; an action that itself may end the nation.

[7] Aaron Mehta, "Nuclear Posture Review Draft Leaks," Defense News, January 12, 2018, https://www.defensenews.com/space/2018/01/12/nuclear-posture-review-draft-leaks-new-weapons-coming-amid-strategic-shift/
[8] Michael Mazarr, "Understanding Deterrence", RAND Corporation, 2018, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf
[9] NPR p. 57
[10] NPR p.31

Absent an imminent nuclear threat, the threshold for use of nuclear arms cannot morally be reached. The NPR's mention of non-nuclear strategic attacks on the NC3 system are telling in what may be perceived as an imminent threat. "It is the perceptions of the potential aggressor that matter, not the aggressor's actual prospects for victory or the objectively measured consequences of an attack."[11] Cyber and space attacks upon circuits and sensors enabling the NC3 system it may be perceived as an act of operational preparation of the environment which signals an attack is imminent. "For decades, the United States has deployed low-yield nuclear options to strengthen deterrence and assurance. Expanding flexible U.S. nuclear options now, to include low yield options, is important for the preservation of credible deterrence against regional aggression."[12] In the event nuclear forces are in the blind it is much easier to consider nuclear first strike which may be conducted with a low yield munition as a form retaliatory messaging while showing restraint.

Conclusion

"What we want to do is to deter. Nobody wants to have a war. The only thing more expensive than deterrence is actually fighting a war, and the only thing more expensive than fighting a war is fighting one and losing."[13]

U.S. Army Chief of Staff, General Mark A. Milley, 2016

U.S. and general world opinion favor a nuclear weapon free world, as such our nation must consider nuclear attack as a last resort effort to preserve our way of life. "Deterrence is best accomplished through broad-based strategies to dissuade a potential aggressor from seeing the need or opportunity for aggression."[14] As such, there is no clear flow graph to follow on when to employ nuclear arms to counter non-nuclear strategic threats, but our willingness to employ in

[11] RAND p.7
[12] NPR p. 54
[13] NPR p.51
[14] RAND p.11

extremis must be explicit. Each moment in time must be evaluated as a whole of the diplomatic, intelligence, military, and economic (DIME) landscape of both the U.S. and the hostile nation.

It would be unwise of an adversary to engage in cyber warfare on a nations NC3 systems unless they explicitly intend on carrying out their own first strike. Presence of malware or any adversary activity on a NC3 system will cause leaders to lose faith in their sensors and make judgements outside of standard rational. Arms control must no longer focus on nuclear arms alone, but on space and cyber weapons as well, but that is challenging on a world stage. The United Nations Committee on the Peaceful Uses of Outer Space (COPUOS) and Prevention of an Arms Race in Outer Space (PAROS) are where action needs to begin. The European Union proposed a Responsible Use acts, China and Russia have proposed Treaty for the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects (PPWT), both of which the U.S. has opposed. "Leadership today is measured not by what we can do alone but what we can get others to do with us."[15] U.S. unwillingness to engage on policy while doubling down on cross domain nuclear threats will only serve to degrade the deterrent value of our nuclear arsenal.

[15] Pace, S. Space 2.0: U.S. Competitiveness and Policy in the New Space Era, Hudson Institute Speech 30 Apr 2018

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D

Cross-Domain Dynamics and the Effect on Aggression, Escalation, and Deterrence in a Nuclear Environment

Capt Steven Bourdow
Dec 21, 2021

Description: The space and cyber domains are becoming increasingly intertwined in both conventional and theoretical nuclear conflicts, disrupting traditional strategies involving aggression, escalation, and deterrence.

Details: Established deterrence and escalation strategies face a significant dilemma: the space and cyber domains. With many spaces and cyber-based assets dual tasked with conventional and strategic missions in domains without accepted behavioral norms, these interactions are not well-bounded or predictable. Kinetic and non-kinetic attacks in these novel domains have the potential for both conventional and strategic effects, begging the question of the adversary's intentions. The goal of this research project is to determine how these cross-domain dynamics affect existing deterrence posture and escalation management strategy. ***Is U.S. deterrence effective in deterring space and cyber-attacks? What actions in these novel domains would result in an event significant enough to warrant U.S. kinetic response – and could that include crossing the nuclear threshold?***

The twenty first century has brought about numerous technological advances to countries across the world. These technologies continue to develop and present new areas of concern for the US and its deterrence strategies. The advances in the space and cyber domains have brought to light the importance of their incorporation into US deterrence strategy. Current strategies face a dilemma in how to incorporate these two domains as assets in both are dual tasked with conventional and strategic missions. More so, neither of these domains have established norms leading to a lot of uncertainty, presenting a potential advantage to adversaries as their intentions become more unknown. Due to this uncertainty any adversary actions, kinetic or non-kinetic, are likely to have both conventional and strategic effects. Currently US space deterrence strategy has not reached the level of effectiveness with deterrence it hopes to achieve based on its Defense Space Strategy.[1] It is also important to point out that both space and cyber domains play a role in nuclear deterrence and the escalation of nuclear weapons threshold. This paper seeks to answer the questions that will inevitably come into play as more actors become involved in the space and cyber domains. First, how can aggression be measured across the space domain that influences nuclear deterrence? Second, what strategies exist to manage escalation and improve deterrence? Lastly, how might the US incorporate an aggression framework for space and cyber domains into the nuclear threshold? For the purposes of this paper, I will be considering the cyber domain as compartmentalized within the space domain for my analysis. The reason behind this is that the cyber domain realistically does not exist without the utilization of the space domain to disseminate the information to the other domains. Therefore, I will primarily address the space domain with cyber considerations built into the context of my analysis. Prior to analyzing each of the focus areas it is important to understand what objectives adversaries, such as China, hope to gain.

[1] Department of Defense, "2020 Defense Space Strategy Summary," 2020, 18.

Current Chinese objectives are to maintain and enhance their international security.[2] The Chinese seek to congest, contest, and make the space domain competitive in pursuit of their goals. They can do this using such things as counterspace capabilities, commercial sector, and government organization. The use of counterspace capabilities to include laser systems, anti-satellite weapons, jamming systems and cyber-attacks with attribute to the congestion of space. The congestion of space then leads to the increase of debris in space, which is a serious topic of discussion amongst space actors. The increase in debris presents a big problem to US nuclear early warning satellites which play a key part in de-escalating nuclear thresholds. The lack of such systems for use escalates the potential for nuclear weapons use given Chinese space weapon use that may or may not be directed near or at one of our national technical means satellites. The contested nature of space that China seeks surrounds the notion that multiple countries treat outer space as a warfighting domain. This outlook opens the potential for an asymmetric approach, which completely differs from the symmetric approach of the Cold War era. This in turn creates greater challenges to deter activities towards nuclear deterrence because activities in space and cyber domains are not all or nothing. This classification of space as a warfighting domain promotes the use for the development of dual use technologies, some of which can be space weapons which attribute to nuclear thresholds. The lack of norms in space also does not allow for attribution of potential weapons built into satellites, which increase the challenge for a tailored deterrence strategy. The competitive nature that China seeks to create in space will cause its commercial and scientific activities more prominence thus extending competition to economic and diplomatic sectors. This again puts the US in a bind because there will be multiple areas where they need to play catch up to prevent China from gaining an advantage. It is important to analyze capabilities that affect the nuclear threshold that could attribute to Chinese security and US deterrence strategy.

Current counterspace capabilities that are possessed by the US, China and other countries seek to deter adversary actions, which likely reflect preventing nuclear escalation and all out nuclear war. Therefore, it can be said that these counterspace capabilities, commonly referred to as space weapons, play a factor in nuclear escalation management. These weapons present challenges to friendly and adversary countries with their variety of capabilities for flexible deterrence. They consist of non-kinetic physical, kinetic physical, electronic, and cyber.[3] Each of these capabilities has its own set of challenges when it comes to attribution and appropriate responses. Non-kinetic physical space weapons create effects on satellites and ground stations without any sort of physical attribution. We see this commonly with lasers or high-powered microwaves that dazzle or blind at satellites sensors, thus making it ineffective.[4] Kinetic physical weapons are the common type of weapon that comes to mind with those that detonate near a ground system or a satellite. We saw this recently with Russia's test in November with their anti-satellite test. This type of weapon is attributable which allows for a way to gauge potential

[2] Kevin Pollpeter, "China's Role in Making Outer Space More Congested, Contested, and Competitive," September 27, 2021, https://www.airuniversity.af.edu/CASI/Display/Article/2789413/chinas-role-in-making-outer-space-more-congested-contested-and-competitive/.

[3] Todd Harrison, Kaitlyn Johnson, and Makena Young, "Defense Against The Dark Arts In Space," n.d., 53.

[4] Robert Preston et al., *Space Weapons Earth Wars* (RAND Corporation, 2002), https://www.rand.org/pubs/monograph_reports/MR1209.html.

adversary aggression/objectives. Electronic weapons utilize the electromagnetic spectrum to interfere with the signal that is received and set by the satellite and is typically referred to as a jammer. Again, like the non-physical weapons this is difficult to attribute where the jamming signal comes from. Lastly cyber-attacks present the potential for the highest chance to increase nuclear escalation. Cyber-attacks will likely have secondary and tertiary effects across all domains as space is inherently linked to them. These attacks are likely to be used in conjunction with attacks in other domains to best set conditions for adversary follow on actions. This then allows for a multidomain approach for an adversary to lower the nuclear threshold and tempt the US and our allies to use nuclear weapons, ultimately starting a global conflict. Based on the counterspace capabilities described above, a framework for determining space aggression provides the means to build a flexible deterrence strategy.

To deter nuclear escalation in space a way to categorize aggressive actions is needed. Herman Khans three types of deterrence provide a general baseline on potential way to categorize aggression. This categorization is broken out into a tiered system that consists of moderate to significant impacts to nuclear deterrence. The first of the tiers is deterrence against a direct attack, second deterrence of extreme provocation, and lastly deterrence of moderate provocation.[5] To clarify, extreme resembles an action, such as space nuclear attack/detonation that results in global turmoil, whereas moderate resembles prolonged actions. The first two tiers can be characterized as passive and active deterrence. The third tier characterizes a more back and forth mentality during prolonged actions. To further see the benefit of the tiered system for space weapon categorization it is important to see how the US could use this categorization.

The first tier of deterrence against a direct attack would constitute the posturing of US space assets from a variety of capable launching sites. This tier also constitutes the public declaration of zero tolerance for the interference/attacks on space systems. The actions within this tier would implicate adversary planning for strategic deterrence. The second tier of deterrence against extreme provocation requires multi-domain capabilities to combat adversary counterspace capabilities. These multi-domain capabilities provide the security and stability for US instruments of national power while simultaneously adding friction and uncertainty to adversaries' decision-making. Like points in the NPR, these multi-domain capabilities would require the inclusion of some type of triad to ensure survivability.[6] The third tier of deterrence against moderate provocation constitutes jamming, interference and intercepting based counterspace capabilities. Keeping those three tiers and associated responses a potential ladder for aggressive activities in space may look like the following:

[5] Herman Kahn, "The Nature and Feasibility of War and Deterrence" (RAND Corporation, January 1, 1960), https://www.rand.org/pubs/papers/P1888.html.
[6] Christopher Stone, "The Space Review: Rethinking the National Security Space Strategy: Part 3 (Page 1)," accessed August 5, 2021, https://www.thespacereview.com/article/2918/1.

1. Non-Interference/Peaceful Use of Space

1. Freedom of Action in Space (civil, commercial, military use of space for benefit of nation and world)
2. Intelligence/SSA Collections (Passive/Active)

2. Reversible, Yet Purposeful Interference Threshold (Deny/Degrade)

1. Passive Jamming
2. Active Jamming/Cyber Attacks
3. Laser Tracking/Dazzling
4. Unauthorized, Rendezvous and Proximity Operations Near U.S. or allied spacecraft
5. Posturing/Mobilization of Destructive Space Attack Forces

3. Irreversible, Purposeful Interference Threshold (Damage)

4. High Energy Chemical Laser
5. High Power Microwave Weapons Use

6. Kinetic, Debris Generation Threshold (Destroy)

1. KE ASAT missiles (Terrestrial Based-LEO)
2. KE ASAT weapons (Co-Orbital)
3. KE ASAT missiles (Terrestrial Based-GEO)

7. Nuclear Use Threshold (Destroy)

1. Terrestrial Fractional Orbital Bombardment Systems (FOBS)
2. Orbital Electro-Magnetic Pulse (EMP)
3. Orbital Nuclear Strike against spacecraft (all orbital regimes affected)

Figure 1: Aggression Escalation Ladder[7]

This figure illustrates an escalation framework on how actions in space may be characterized. As actions flow down the ladder depicted here, the effects increase causing an increase in nuclear escalation. Within this ladder, areas that may constitute a likely US kinetic or non-kinetic response are any of those actions above falling under the damage or destroy category as those are likely to have the biggest impact on nuclear escalation. A manner to proactivity control escalation levels and deter adversary activities is using active and passive defense strategies.

[7] Christopher M. Stone, "The Space Review: Rethinking the National Security Space Strategy: Part 3 (Page 2)," accessed November 16, 2021, https://www.thespacereview.com/article/2918/2.

The unique complexities of deterring in space create complex challenges. One such challenge is how to keep nuclear escalation levels low while simultaneously deterring enemy actions. One potential answer to this challenge is with active and passive defense strategies. Both strategies provide the capabilities and capacities to respond to a wide range of threats within the current and future proliferation of space. In this manner the US would have the ability to protect friendly systems and capabilities to disrupt, degrade, or destroy adversary systems. The perception of these types of defenses could be taken as a form of offensive strategy, which may then raise red flags to other countries that the US is conducting escalatory actions, but according to international laws these strategies fall within its bounds.[8] The analysis of these defensive capabilities below allow for parallel operations with one another across passive and active defenses, aiding in the bolstering of nuclear de-escalation and deterrence.

To begin we will take a dive into passive defense capabilities that will minimize the effectiveness of adversary attacks and make US space systems, to include missile warning capabilities, more resilient. Within the framework of passive measures three areas will be analyzed for strategic use: architecture, technical, and operational. Architectural surrounds the space and ground segments of space systems, technical the technologies that may be incorporated across all domains, and operational the way space systems are operated. Each of these strategies for passive defense are capable of working independently, but for the best possible outcome, the amalgamation of all three provides the best capabilities and opportunities for deterrence.

The architecture portion within the passive defense framework primarily focuses on the organization of different satellite constellations. These organizations consisting of disaggregated, distributed, proliferated, and diversified constellations contribute to deterring adversary actions. Disaggregation involves separating the multiple mission set of one satellite into separate mission specific satellites capable of operating in parallel with one another. In a conventional conflict if an adversary targets strategic and tactical use satellite it becomes unclear as to what use case the adversary intended to target which then may cause unintentional escalation. Disaggregated constellations do separate our tactical and strategic use satellites, meaning an adversary could target a tactical use satellite without risking nuclear escalation. However, the adversary may not be able to distinguish the intended mission for a specific satellite in this constellation creating uncertainties for the adversary if they do not wish to increase escalation. Distributed constellations consist of a number of satellites acting as nodes where all are able to perform the same function. This architecture complicates adversary decision making for counterspace activities as there are multiple targets that would need to be attacked in order for the effects they desire to be achieved. Distributed satellites are also capable of hosting payloads from other countries or commercial actors further putting an adversary in a dilemma if they are willing to potentially attack another country. Proliferated constellations consist of a large number of satellites that are all in similar orbits and perform the same mission set. This type of architecture is capable of providing increased protection because of the sheer number of satellites in orbit. For an adversary to reach its desired effects it may need to attack all of the satellites in the

[8] Harrison, Johnson, and Young, "Defense Against The Dark Arts In Space."

constellation, which would likely result in a significant amount of money spent for minimal results and potential diplomatic sanctions. Lastly, diversified architectures represent multiple systems spread throughout various orbits that possess the same mission sets or potentially different domains, i.e., cyber. The diversification of these systems reduces potential adversary attacks as there is not much incentive in attacking a system when others in different orbits or domains can fulfill the mission. A potential approach an adversary may take to overcome these different architectures is the use of different counterspace capabilities like those discussed above, however, there is an increased probability of collateral damage, orbital debris, which are likely to result in greater impacts in diplomatic and economic global relations, running the risk of increasing escalation. These architectures are just but one piece of the pie that contributes to passive measures contributing to deterrence.

A second type of strategy surrounding passive defense measures is through the use of technical defenses. These technicalities provide increased opportunities for the previously stated architectures to flourish within a cloak of deterrence. Some technical aspects that contribute to increased opportunities are Space Domain Awareness, radio frequency mapping, electromagnetic shielding, shuttering, and jam resistant waveforms. These capabilities provide the means to gather information, characterize potential adversary capabilities or likely actions and reinforce US satellites from attacks on electronics or telemetry subsystems. Much like the architectures this variety of capabilities presents a complex set of areas for the adversary to concern itself with, which will likely increase uncertainty, slow down their decision making process and make them question if actions to attack are worthwhile. It is important to note that these technical actions also have an effect on the US. More robust technical capabilities result in greater costs, larger systems, and longer timelines for procurement then launch. This illustrates the balancing act that comes into play when implementing said technical aspects into a flexible deterrence strategy. The potential operational defenses that may be implemented further the trickiness of this balancing act.

A third type of strategy to use falling under passive measures is operational defense. This type of strategy focuses on making satellites harder to target, more resilient to attacks or easier to replace in the event of an attack. Areas that fall under the strategic objectives are rapid deployment, reconstitution, maneuver, stealth, and deception and decoys. In a similar fashion to World War II, these operational concepts could be implemented to disorient and confuse the adversary on what approach it wants to pursue to meet its objectives, leading to greater lead time for their decision making, increasing opportunities to deter through other domains. Much like the technical defense strategy there are constraints built in. Launching satellites is constrained to certain windows of time, the cost of replacing satellites rapidly may take away from other opportunities to deter, and once satellites are in orbit there is a finite amount of fuel on board so maneuvers will not need to implicate future mission requirements. This operational approach while it does present advantageous avenues to pursue for deterrence will drive the strategy the strategy of the technical and architectural defenses. All three passive strategies are interconnected and may rely on one or the other for deterrence based effects. These strategies must also be looked at for parallel use with active defense.

The strategy of active defense centers on targeting an adversary threat system. Space Force doctrine adheres to the use of active defense. While this may lead to potential reactive activities from adversaries, it also allows for the US to be proactive with the seizing an initiative to prepare for a potential attack. Active defense strategy is broken down into two categories space-based and terrestrial-based. Like both categories alluded to each is focused on techniques and procedures to protect space assets in both areas. Many of the capabilities discussed above on the different types of counterspace capabilities fall within the realm of active defense strategies. Depending on the threat the adversary presents there is a capability that could be pre-positioned and used in a flexible manner to deter any actions. With that being said adversary's have the capabilities to do the same thing to us, which could cause a stalemate. Inadvertently this could potentially create deterrence effects as neither the US nor its adversary take any actions that might undermine nuclear stability. In addition to undermining nuclear stability, the use of counterspace capabilities in active defense strategies also increases the opportunities for orbital debris causing second and third order effects to friendly and allied systems. Based on the current international climate with debris mitigation, actions resulting in increased debris creation may lead to other nations perceiving those actions as escalatory. While that might be a stretch, we see the implications that the Russians caused with their most recent antisatellite test last month creating debris almost causing major ramifications for the International Space System. Collectively, the strategies of both passive and active defense bring pros and cons to the table when it comes to deterrence. In this analyst's opinion it is necessary to have a little bit of both strategies in play because it brings in deterrence by denial and deterrence by punishment. The strategy then allows for flexible deterrent options that may be tailored to the adversary or the threat they present. It is with this that the US may deter any potential actions that cross would the nuclear threshold.

To determine if a US kinetic or non-kinetic response is warranted it would help to see what areas the ladder for aggressive actions from above falls under within nuclear thresholds. Within the NPR nuclear threshold is defined as a point in a conflict at which nuclear weapons are or would be brought into use.[9] From the screenshot below we see the different levels that contribute to the escalation of nuclear thresholds.

[9] "2018 Nuclear Posture Review," accessed November 20, 2021, https://dod.defense.gov/News/SpecialReports/2018NuclearPostureReview.aspx

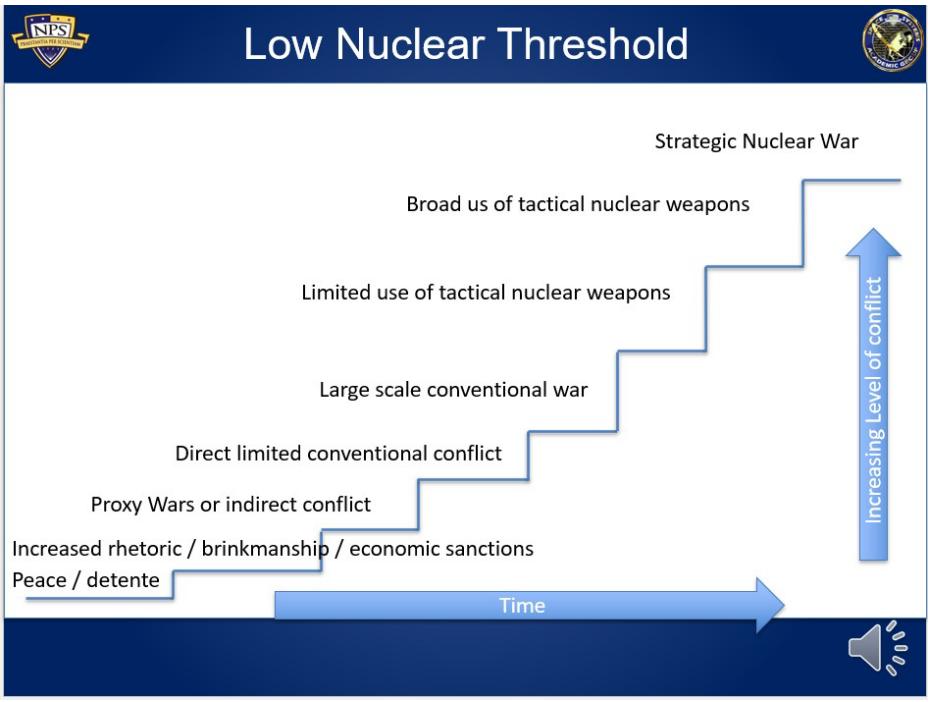


Figure 1: Nuclear Threshold[10]

Based on the aggression framework above non-interference/peaceful uses of space would fall under the peace/détente portion of nuclear thresholds. These space actions constitute daily operations and the betterment of space, so the likelihood of nuclear activities is low. Reversible, yet purposeful interference, deny/degrade operations, would fall under the proxy wars or indirect conflict umbrella of nuclear threshold. Those activities such as jamming, dazzling, rendezvous or posturing space capabilities are likely used to inhibit space actor's actions. Being reversible in nature allows for the incremental starting and stopping of interference which may then steer decision-making processes of those involved to limit or shift their ideologies on space. The irreversible, purposeful interference with intent to destroy would likely fall under a directed limited conventional conflict umbrella. The reasoning behind this is because if the US can accurately attribute adversary actions, then it can respond with non-kinetic capabilities in a similar fashion. This could be characterized as a tit for tat type of conflict where the US and its adversary do little things here and there to implicate one another. Kinetic actions that result in debris, such as anti-satellite weapons tests, I would argue also fall under the umbrella of a direct limited conventional conflict. The recent Russian anti-satellite test resulted in a significant amount of debris that affected the International Space Station and other satellites within that orbital regime, however, there has yet to be any actions take on Russia outside of further debates surrounding debris mitigation. If this action were taken on a US or ally space system, I would see the reasoning for a US kinetic response. The decision on whether it constitutes crossing the nuclear threshold is dependent on if the system being attacked is a strategic, operational, or tactical level asset. Another difficulty in determining if a US kinetic response is warranted is the fact that there are not a common set of norms and behaviors agreed on by space actors. This

[10] Crook.

complicates appropriate responses as different viewpoints from adversaries may result in the crossing of the nuclear threshold and use of nuclear weapons. One such action that would result in the crossing of the nuclear threshold are any activities surrounding bombardment systems, electromagnetic pulses, or nuclear attacks on space systems. These actions would cause cascading effects on the environment and worldwide use of space for those actors involved. This would have serious ramifications on the capabilities across all domains implicating terrestrial operations. Therefore, in this case it would warrant a US kinetic response that crosses the nuclear threshold as the entire space domain is significantly affected resulting subsequent effects on terrestrial domains. At this point the likelihood of strategic nuclear war may be feasible as tensions across the globe have increased with diplomatic, information, military and economic sanctions against the actor that took the initial action. Again, the response the US would take against such an action are likely dependent on appropriate behaviors in space and norms.

Collectively space and subsequent cyber domain present challenges to US deterrence strategy, especially as technology rapidly evolves. The various types of space weapons and their effects create a variety of ways in which the US could tailor their strategy. The basic framework as discussed above gives a general starting point for the US to look at different levels of aggression pending the effects achieved. This framework also allows for the initial categorization of what areas within the nuclear threshold these levels of aggression fall under. These characterization and categorizations of aggression and nuclear threshold levels allow for the flexibility in deciding what type of deterrence strategies to use, active, passive or combination of the two. Current US deterrence strategy is not to the level it would like to be with deterring adversary attacks; however, this is likely a root cause of the limited agreements on appropriate behaviors and norms for space itself. As now it stands the escalation of nuclear weapons use remains low, but one drastic action from any actor in space could light the fuse to drive past that threshold.

Bibliography

"2018 Nuclear Posture Review," accessed November 20, 2021, https://dod.defense.gov/News/SpecialReports/2018NuclearPostureReview.aspx

Department of Defense. "2020 Defense Space Strategy Summary," 2020, 18.

Harrison, Todd, Kaitlyn Johnson, and Makena Young. "Defense Against The Dark Arts In Space," n.d., 53.

Kahn, Herman. "The Nature and Feasibility of War and Deterrence." RAND Corporation, January 1, 1960. https://www.rand.org/pubs/papers/P1888.html.

Pollpeter, Kevin. "China's Role in Making Outer Space More Congested, Contested, and Competitive," September 27, 2021. https://www.airuniversity.af.edu/CASI/Display/Article/2789413/chinas-role-in-making-outer-space-more-congested-contested-and-competitive/.

Preston, Robert, Dana J. Johnson, Sean J. A. Edwards, Michael D. Miller, and Calvin Shipbaugh. Space Weapons Earth Wars. RAND Corporation, 2002. https://www.rand.org/pubs/monograph_reports/MR1209.html.

Stone, Christopher. "The Space Review: Rethinking the National Security Space Strategy: Part 3 (Page 1)." Accessed August 5, 2021. https://www.thespacereview.com/article/2918/1.

Stone, Christopher M. "The Space Review: Rethinking the National Security Space Strategy: Part 3 (Page 2)." Accessed November 16, 2021. https://www.thespacereview.com/article/2918/2.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E

Cross-Domain Dynamics and the Effect on Aggression, Escalation, and Deterrence in a Nuclear Environment

Major Isaac Williams
Fall QTR 22

Naval Postgraduate School
SS3740 – NC3 Part I

Introduction

In 1954, the United States (U.S.) was deep into testing thermonuclear capabilities at the Bikini Atoll in the Marshall Islands with a 15 megaton (MT) bomb called Shrimp.[1] Conversely, the U.S. was still in the infant stage of understanding the range of destruction that a nuclear bomb would make as well as what type of destruction (i.e., thermal, physical, or radiation). Consequently, 80 miles from the test, a Japanese fishing crew and their catch were exposed to radiation which they unknowingly brought back to Japan.[2] While this did create some global social conundrums for the U.S., "the entire national security policy of the United States now depended on its nuclear weapons."[3] As a result, the Cold War saw an increase in nuclear production to alarming numbers. However, since the 1990s the U.S. and allies have increased efforts to reduce the total number of nuclear warheads while still maintaining a confident level of deterrence. In fact, "U.S. nuclear weapons not only defend our allies against conventional and nuclear threats, but they also help them avoid the need to develop their own nuclear arsenals."[4] Yet, while the U.S. is moving one direction— efforts to eliminate weapons of mass destruction (WMD)— Russia and China are moving the other way. To complicate matters beyond nuclear weapons, cyberweapon advancement and counterspace capabilities have increased with an interlinked mutually supporting relationship. With these factors in play, the U.S. should not remain solely focused on a deterrence posture and escalation management strategy revolving around nuclear weapons but create, adopt, and sustain a true multi-domain deterrence policy. This paper will address cross-domain dynamics in the existing deterrence posture and escalation management strategies, explain how the space-cyber link affects deterrence related to our nuclear posture, explore how cyber-space escalation could lead to nuclear aggression, and cite potential improvements to the deterrence posture.

Existing Deterrence Posture and Escalation Strategies

To begin the first point of addressing modern cross-domain dynamics it is important to grasp a novice understanding of deterrence by analyzing current deterrence posture and escalation strategies. According to the 2018 Nuclear Posture Review (NPR), the U.S. does not want to consider "Russia or China as an adversary and seeks stable relations with both."[5] The fact of the matter remains that Russia and China are creating geopolitical problems by increasing nuclear weapon capabilities and upsetting the international norms by overstepping the sovereignty of bordering nations. These facts make it very hard to reach a goal of stable relations when China and Russia act like adversaries, which leads to the need of maintaining and modernizing our nuclear triad. The triad is comprised of submariners (SSBN), land based intercontinental ballistic missiles (ICBM), and strategic bombers carrying gravity bombs and air-launched cruise missile (ALCM). Least of all, the triad is held together by the Nuclear, Command, and Control (NC3) system comprised of satellites, radars, and ground control stations. Additionally, the U.S. allies in Europe, Asia, and the Pacific create an assurance common goal to deter or defeat threats that we may face which strengthen our extended

[1] Schlosser, Eric. *Command and Control*. The Penguin Press, 2013.
[2] Ibid.
[3] Ibid.
[4] Office of the Secretary of Defense. (February 2018). *Nuclear Posture Review.*
[5] Ibid.

deterrence posture.[6] These tools are part of the "nuclear deterrence tool-bag" as they assist in meeting the end goal of stable relations.

One of the best ways to eliminate escalation ambiguity is to be blunt up front. As stated from the 2018 NPR,

> Potential adversaries must recognize that across the emerging range of threats and contexts:
>
> 1) The United States is able to identify them and hold them accountable for acts of aggression, including new forms of aggression.
> 2) We will defeat non-nuclear strategic attacks.
> 3) Any nuclear escalation will fail to achieve their objectives and instead result in unacceptable consequences for them.[7]

These three factors about the U.S. deterrence posture and escalation strategy could be summed up into one statement, "deterrence is just deterrence."[8] While it was true during the Cold War that nuclear strategy was the foundation of deterrence policy, the unfolding revelation in the present day is "nuclear weapons are a deterrent, not the deterrence itself."[9] Meaning cyberwarfare and counterspace cross-domain dynamics have the potential of escalating nuclear retaliation against non-nuclear attacks. Compounding factors of employing nuclear weapons requires a multi-domain approach because the nuclear weapon system encompass all domains even more so in the present day. This leads to another potentially true statement regarding the 2018 NPR, "the domain is irrelevant because deterrence is a concept that includes all types of tools."[10]

Fast forward from the 2018 NPR to the present-day presidential administration, a change to the deterrence posture and escalation strategy is a spaghetti plate of buzzwords piled high on the integrated deterrence dinner plate. According to Secretary of Defense (SECDEF) Lloyd J. Austin, "integrated deterrence is the right mix of technology, operational concepts, and capabilities – all woven together in a networked way that is so credible, and flexible, and formidable that it will give any adversary pause…[and] is multi-domain, spans numerous geographic areas, is united with allies and partners, and is fortified by all instruments of national power."[11] First of all, integrated deterrence appears to be more of problem statement than a solution. Second, if this definition means that deterrence is integrated, does that mean that whatever the U.S. was doing before was not integrated? Third, "give any adversary pause…" does not sound like a statement that is making an effort to stop or prevent an action, as opposed to the closely related but distinct concept of "compellence," which is an effort to force an actor to do something.[12] Fourth, there is a lot of emphasis on allies and partners being included in this deterrence posture which means that they need to be committed to the cause of integrated

---

[6] Ibid.
[7] Office of the Secretary of Defense. (February 2018). *Nuclear Posture Review.*
[8] Petrucci, N. (2018, December 1). *Building "Space" Into Multi-Domain Deterrence Strategy.* Air Power Strategy. http://www.airpowerstrategy.com/2018/12/01/space-deterrence/.
[9] Ibid.
[10] Ibid.
[11] Ullman, H. (2021, November 12). *Integrated Deterrence: Buzz Words Or a Bold Idea?* U.S. Naval Institute Blog. https://blog.usni.org/posts/2021/11/12/integrated-deterrence-buzz-words-or-a-bold-idea.
[12] Mazarr, Michael J. (2018). *Understanding Deterrence.* RAND Corp. www.rand.org.

deterrence and/or pull their weight. And lastly, SECDEF Austin also emphasized that investment changes and innovation requirements will need to occur in all domains to develop new ideas.[13] This sounds like this administration is going to turn their focus to economic or diplomatic means of deterrence instead. This could potentially mean that the Department of Defense (DoD) budget will decrease which could affect the nuclear triad modernization requirements listed in the 2018 NPR. Regardless of where the deterrence posture is headed, this administration still understands that cross-domain dynamics are involved with nuclear capabilities.

The Space-Cyber Nuclear Deterrent Relationship

Speaking of domains, a multi-domain race has emerged in the form of vast commercialization, increased militarization, and potentially new weaponization techniques and technology. Space technologies, pursued successfully from a couple powerful countries, now has the appearance that almost anyone with a rocket kit can put satellites in space. Consequently, this also means that the risk to the U.S satellite architecture is increasing from those who may want to do harm. As it is common knowledge, the U.S. military is highly reliant on satellites for communication, intelligence, surveillance, reconnaissance (ISR); position, navigation, timing (PNT); beyond line of sight targeting (BLOS); and the NC3 system.

In addition to needing satellites for those capabilities, those capabilities are meaningless without data. Whether the data is being pushed to the user or pulled from the user is irrespective; it is the key to the puzzle of a resilient deterrence architecture. This data exists within the cyber domain through hard wired networks but is increasingly networked using satellites for the purpose of expediting the transmission of data to occur globally. Hence, the space-cyber link is born, "presenting challenges to nuclear stability that deserve more attention than they're getting."[14] In addition, many space and cyber-based assets are dual tasked with conventional and strategic missions in their domains without accepted behavioral norms.[15] Paring this predicament with advancements in cyberweapons and counter-space capabilities are certainly creating new pressures on concepts of nuclear deterrence as traditionally construed.[16]

This predicament is being transposed onto the modernization of its nuclear infrastructure because the weapon systems are increasingly becoming cyber-space reliant. As a result, the NC3 system must be hardened to protect new ICMBs known as the ground-based strategic deterrent (GBSD).[17] This modernization will bring with it faster connectivity and warning within the NC3, but it does not come without risks of increased cyber-attacks to the software or hardware that is being installed. Cyber penetrations of critical infrastructure amount to what the military calls

---

[13] Osborn, K. (2021, July 14). *Defense Secretary Austin Outlines New 'Integrated Deterrence' Strategy.* The National Interest. https://nationalinterest.org/blog/buzz/defense-secretary-austin-outlines-new-%E2%80%98integrated-deterrence%E2%80%99-strategy-189661.

[14] Miller, J., Fontaine, R. (2017, November 26). *Cyber and Space Weapons Are Making Nuclear Deterrence Trickier.* Defense One. https://www.defenseone.com/ideas/2017/11/cyber-and-space-weapons-are-making-nuclear-deterrence-trickier/142767/.

[15] Crook, M. (2021). *SS3740 Final Paper Introduction.* Sakai.

[16] Miller, J., Fontaine, R. (2017, November 26). *Cyber and Space Weapons Are Making Nuclear Deterrence Trickier.* Defense One. https://www.defenseone.com/ideas/2017/11/cyber-and-space-weapons-are-making-nuclear-deterrence-trickier/142767/.

[17] Osborn, K. (2021, November 16). *America's ICBMs Need Better Infrastructure.* The National Interest. https://nationalinterest.org/blog/reboot/americas-icbms-need-better-infrastructure-196381.

"preparation of the battlespace,"[18] which, in turn, can create significant pains through non-kinetic, non-lethal cyber-attacks. This escalation within the space-cyber cross domain could escalate to nuclear aggression.

The Space-Cyber Nuclear Erosion

First, before providing some examples as to how the space-cyber escalation could lead to nuclear aggression, it is also important to understand how China and Russia view deterrence. "Chinese views on deterrence differ significantly from Western view, beginning with greater emphasis on coercion. Their focus isn't so much on deterring actions in the space-cyber realm but coercing an adversary through actions in the space and cyber domain, often in conjunction with conventional and even nuclear forces."[19] This means that counterspace and cyberwarfare can be used to get the U.S. and/or their allies to do something they want to them do. In that case, space and/or cyber are not really domains that are discussed to be essential for deterrence. For example, space weapons for the Chinese are a rung on their escalation ladder of deterrent actions where U.S. space weapons are rarely considered part of deterrence.[20] This difference of opinion could create problems based off the 2018 NPR.

Similarly, Russian views of nuclear weapons in deterrence are different than the U.S. "In Russian, the closest term of deterrence is *Sderzhivanie* – implying active defense. Hence, the Soviets and the Russian Federation concluded that planning for that contingency [retaliation] could not be ignored and must be part of strategy. That meant 'fighting' a nuclear war had to be considered no matter the costs because once a conflict started, survival was existential – a concept foreign to the United States and the West."[21] This implies that first strike from the Russians is still on the table if they believe that the potential conflict is great enough that for them to survive, they will use nuclear weapons.

Russia and China's views on deterrence could present some challenges if they are not interpreted correctly. Being as the U.S. is so reliant on space and cyber, the cyber- or space-attacker could gain military and coercive advantage, while putting the onus on the attacked side to dare escalate with "kinetic" lethal attacks.[22] For example, attacking the U.S. missile warning satellites or cyber networks that are used for our nuclear weapons could create perceptions of an impending nuclear first strike. This means that the U.S. could be led into using serious lethal force from the top of our escalation ladder instead of climbing up it. While neither side should move towards this type of action, China and maybe even Russia could carry out this operation because they are trying to reach a desired action or end state to meet their political goals.

---

[18] Miller, J., Fontaine, R. (2017, November 26). *Cyber and Space Weapons Are Making Nuclear Deterrence Trickier.* Defense One. https://www.defenseone.com/ideas/2017/11/cyber-and-space-weapons-are-making-nuclear-deterrence-trickier/142767/.

[19] Cheng, D. (2016, January 21). *Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC.* The Heritage Foundation. https://www.heritage.org/defense/report/prospects-extended-deterrence-space-and-cyber-the-case-the-prc.

[20] Ibid.

[21] Ullman, H. (2021, November 12). *Integrated Deterrence: Buzz Words Or a Bold Idea?* U.S. Naval Institute Blog. https://blog.usni.org/posts/2021/11/12/integrated-deterrence-buzz-words-or-a-bold-idea.

[22] Miller, J., Fontaine, R. (2017, November 26). *Cyber and Space Weapons Are Making Nuclear Deterrence Trickier.* Defense One. https://www.defenseone.com/ideas/2017/11/cyber-and-space-weapons-are-making-nuclear-deterrence-trickier/142767/.

Not only are these space or cyber-attacks likely to occur on nuclear infrastructure "it is not unreasonable to reach the conclusion that a cyber-attack on critical infrastructure could be deemed an armed attack against which the U.S. could respond with non-cyber means."[23] This is especially true now that the "16 different critical infrastructures" identified by the Department of Homeland Security has been made public to our adversaries.[24] In essence, if an attack on one of these critical infrastructures is serious enough to the U.S. economy or to the sustainment and well-being of the American public, "it could, theoretically, legally merit a nuclear response."[25]

These doomsday scenarios have validity but being as China and Russia view deterrence differently than the U.S., it would benefit the U.S. to measure deterrence in this multi-domain environment where a cyber "spark" does not start a nuclear fight. However, it is becoming increasingly difficult to find the source of a cyber-attack because our adversaries are using third party actors to conduct cyberwarfare. Additionally, counterspace weapons are advancing to the point where their lethal capabilities are harder to detect making the attack non-attributional. As a result, measures of effectiveness are almost an unrealistic way to identify if there is an eroding deterrence posture. To prove the point, listed below are some paraphrased examples of measures of effectiveness as discussed on a podcast by War on the Rocks:

1) Assurance: Through our deterrence actions, find a quantitative way to measure if the U.S. keeps the same number of allies/partners, increases the number of allies/partners, or loses allies/partners.
2) Distinct end states: For example, by 2030 Russia has not invaded Ukraine and China has not tried to reunify Taiwan. If there is a build-up of troops on the Ukraine border or if China is conducting increased military flights over Taiwan, the deterrence posture is eroding.
3) Cyber arms control: While it is difficult to reduce the number of countries that increase capabilities to conduct cyber-attacks, by using the guardrails of global persecution, the U.S. and allies can spotlight those countries by bringing many classified cyber-attacks into the open. If more cyber-attacks are occurring, then your deterrence posture is eroding.

While it would be nice if eroding deterrence polices were simplified by similar measures of effectiveness factors—a deterrence framework is hard to quantify. Instead, the U.S. needs to mitigate erosion by improving deterrence strategies in hopes to manage escalation.

Improvement to Deterrence and/or Strategies to Manage Escalation

Since it has been over 70 years since an atomic bomb was used in warfare, there is increasing inquisitive thought on what future warfare could look like. For example, themaneuverist.org, a website that is dedicated to the warfighter for "…developing military minds of investigative curiosity, analysis, and synthesis…,"[26] has a future vignette of warfare in the Pacific. This is an excerpt from that article:

---

[23] Cal, Nerea. (2018, March 19). *Nuclear Weapons' New Purpose: Deterring Cyber Attacks?* Modern War Institute. https://mwi.usma.edu/nuclear-weapons-new-purpose-deterring-cyber-attacks/.
[24] Ibid
[25] Ibid.
[26] The Warfighting Society Leadership Team. https://www.themaneuverist.org/about-us.

> Three weeks ago, the satellites stopped. Two weeks ago, Internet protocols failed. Last week, a series of enhanced electromagnetic pulses triggered across the Pacific. Within 6 hours, every expeditionary advanced base was bombarded with naval gun fire. Thousands of awakened cannons with nothing to stop them. Your autonomous logistics crafts and small boats became erratic after losing satellites. They are nothing more than silent buoys and anchors now. No one in Washington or Hawaii knew for hours, and by the time they did, it was too late. You see, General, even your redundant systems failed.[27]

This vignette perceives that the U.S. whole of government approach (now called integrated deterrence) is extremely vulnerable and easy for an adversary to overcome the physical, scientific, and political challenges to neutralize and/or destroy our networks through multi-domain operations. This also points to another issue, there is no mention of nuclear weapons being used or being vital to deterring China from creating conflict. When it comes to this large scale of conflict, it would be assumed that nuclear weapons are crucial to prevent an attrition point of view. However, at no fault to these warfighters, you can not properly plan for operations, if the tools you need to deter are in the black, and only a few know about them. This leads to the first point about improving deterrence options, classification. Allowing a larger swath of military planners in on cross-domain deterrence options could allow for refined products, assumptions, and continue the success of not having to use nuclear weapons in great power conflict.

As mentioned earlier, allies and partners are an important part of deterrence. Largely because numbers do matter. The more friends you have backing you up with the same strengths and/or capabilities, the less likely it is that an adversary will mess with you. Additionally, these allies can share intelligence on countries that hinder another countries deterrence. In a similar fashion, situational awareness in space can add to this assurance by knowing where space assets are located. This is done by ground radar stations and satellites in space to let the U.S. know when spy satellites are approaching. Revisiting the idea that data is key - transporting that data at even faster rates makes it more likely that the NC3 system will be hardened from cyber and/or space attacks. The Space Defense Agency (SDA) is trying to solve this problem by creating a transport layer that "hardens the links between space assets and ground stations to be able to command satellites when necessary."[28] This transport layer will be an important aspect of strengthening the deterrence bond between allies and partners if the U.S. creates opportunities for coalition interoperability within the transport layer.

Finally, norms need to be established by all space faring and cyber capable nations when it comes to cross-domain capabilities in space and cyber. Norms are easier to extend than new strategic arms reduction treaties are to negotiate, and nuclear numbers are to reduce.[29] For one thing, speed, stealth, unpredictability, and challenges of attribution of any particular cyberattack make it exceedingly difficult, if not impossible, to anticipate, deter, and defend against all cyber

---

[27] Weibling, Scott., Miller, Jordan, and Tweedy, Matt. "The Ghost & General Smith: Preface and Chapter 1." (Sep 2021). https://www.themaneuverist.org/post/the-ghost-general-smith-preface-and-chapter-1-by-scott-weibling-jordan-miller-and-matt-tweedy.

[28] Petrucci, N. (2018, December 1). *Building "Space" Into Multi-Domain Deterrence Strategy.* Air Power Strategy. http://www.airpowerstrategy.com/2018/12/01/space-deterrence/.

[29] Krepon, M. (2021, November 8). *How to Avoid Nuclear War.* War on the Rocks. https://warontherocks.com/2021/11/how-to-avoid-nuclear-war/.

threats.[30] The continued pursuit of space weaponization must be avoided to eliminate the wrong idea and it must be remembered that space is a global common. Therefore, the most pressing challenge is to bring together nuclear-armed states and seek agreement on preventing the most dangerous dynamics presented by the cyber threats and/or counterspace operations.[31]

Conclusion:

In conclusion, being inquisitive on deterrence in a multi-domain environment is part of being a professional warfighter but having the knowledge to frame it properly is just as important. Nuclear weapons are the most lethal weapons in the world, but these weapons are not invincible. As they continue to be modernized to operate within the 21st century, their reliance on cyber networks and satellites will only increase. This means that they are prone to attacks from across all domains. Even more dynamic is the evolving non-attributional capabilities within the cyberwarfare and counterspace domains that make it difficult to determine the source of the attack. This also makes is difficult to measure the effectiveness of the U.S. deterrence posture. Therefore, mitigations measures by the U.S. and allies should be included with the consistent and persistent review of cyber and space threats to nuclear weapons systems. As stated from the Nuclear Threat Initiative, "Perhaps more important, governments must be willing to question the continued viability of nuclear deterrence strategy, asking whether it is just a word salad passed from one administration to the other or if it is becoming obsolete."[32] Finally, being aggressive but realistic is a key aspect to the U.S. deterrence posture, eloquently stated by Petrucci, "A multi-domain deterrence policy hinges on unaffordable outcomes. Projecting a true multi-domain deterrence policy to hold retaliation in all domains ensures any missteps in the space and/or cyber domain can be dealt with at the time and place of the U.S. choosing."[33]

---

[30] Stoutland, P., Pitts-Keifer, S. (2018, September). *Nuclear Weapons in the New Cyber Age.* Nuclear Threat Initiative. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fmedia.nti.org%2Fdocuments%2FCyber_report_finalsmall.pdf&clen=2184667&chunk=true

[31] Stoutland, P., Pitts-Keifer, S. (2018, September). *Nuclear Weapons in the New Cyber Age.* Nuclear Threat Initiative. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fmedia.nti.org%2Fdocuments%2FCyber_report_finalsmall.pdf&clen=2184667&chunk=true.

[32] Ibid.

[33] Petrucci, N. (2018, December 1). *Building "Space" Into Multi-Domain Deterrence Strategy.* Air Power Strategy. http://www.airpowerstrategy.com/2018/12/01/space-deterrence/.

Bibliography

Cal, Nerea. *Nuclear Weapons' New Purpose: Deterring Cyber Attacks?* 19 March 2018. 15 November 2021. <https://mwi.usma.edu/nuclear-weapons-new-purpose-deterring-cyber-attacks/>.

Cheng, Dean. *Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC*. 21 January 2016. 14 November 2021. <https://www.heritage.org/defense/report/prospects-extended- deterrence-space-and-cyber-the-case-the-prc>.

November 2021. Defense, Office of the Secretary of. "National Posture Review." 2018.

Fontaine, James Miller and Richard. *Cyber and Space Weapons Are Making Nuclear Deterrence Trickier*. 26 November 2017. 16 November 2021. <https://www.defenseone.com/ideas/2017/11/cyber- and-space-weapons-are-making-nuclear-deterrence-trickier/142767/>.

Krepon, Michael. *How to Avoid Nuclear War*. 8 November 2021. 15 November 2021. <https://warontherocks.com/2021/11/how-to-avoid-nuclear-war/>.

Mazarr, Michael J. *Understanding Deterrence*. 2018. 15 November 2021.

Osborn, Kris. *America's ICBMs Need Better Infrastructure*. 16 November 2021. 16 November 2021. <https://nationalinterest.org/blog/reboot/americas-icbms-need-better-infrastructure-196381>.

—. *Defense Secretary Austing Outlines New 'Integrated Deterrence' Strategy*. 14 July 2021. 15 November 2021. <https://nationalinterest.org/blog/buzz/defense-secretary-austin-outlines-new-%E2%80%98integrated-deterrence%E2%80%99-strategy-189661>.

Petrucci, Nicole. *Air Power Strategy*. 1 December 2018. 1 November 2021. <http://www.airpowerstrategy.com/2018/12/01/space-deterrence/>.

Pitts-Kiefer, Page Stoutland and Samantha. *Nuclear Weapons in the New Cyber Age*. September 2018. 15 November 2021.

Schlosser, Eric. *Command and Control* . New York: The Penguin

Press, 2013. Team, The Warfighting Society Leadership. *About*

Us. n.d. November 2021.

Tweedy, Scott Weibling and Jordan Miller and Matt. *The Ghost & General Smith: Preface and Chapter 1*. September 2021. November 2021.

Ullman, Harlan. *Integrated Deterrence: Buzz Words Or a Bold Idea?* 12 November 2021. 15 November 2021. <https://blog.usni.org/posts/2021/11/12/integrated-deterrence-buzz-words-or-a-bold- idea>.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Research Sponsored Programs Office, Code 41
   Naval Postgraduate School
   Monterey, CA 93943