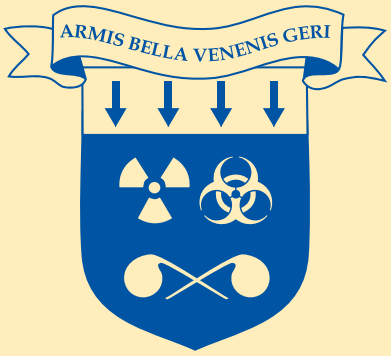
Non-U.S. Deterrence Strategies: What Must the United States Be Prepared For? AY19 Strategic Deterrence Research Papers (Vol II)

Edited by:
Dr. Paige P. Cone
Dr. James Platte
Dr. R. Lewis Steinhoff



United States Air Force
Center for Strategic Deterrence Studies
Maxwell Air Force Base, Alabama

Non-U.S. Deterrence Strategies: What Must the United States Be Prepared For? AY19 Strategic Deterrence Research Papers (Vol II)

Edited by

Dr. Paige P. Cone

Dr. James E. Platte

Dr. R. Lewis Steinhoff

U.S. Air Force Center for Strategic Deterrence Studies
125 Chennault Circle
Maxwell Air Force Base, Alabama 36112

October 2019

Table of Contents

Disclaimer

The views expressed in this academic research paper are those of the individual authors and do not reflect the official policy or position of the United States government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Preface

During the Academic Year 2019, the U.S. Air Force Center for Strategic Deterrence Studies (CSDS) provided a Deterrence Research Task Force (DRTF) elective for Air War College and Air Command and Staff College students. Of the students, 17 (11 from the Air War College and six from the Air Command and Staff College) with broad and diverse backgrounds participated in this course. They engaged in critical thinking about the nature of strategic deterrence and the role of nuclear weapons under strategic deterrence policy. The class took two field trips: one to Washington, D.C., to engage with staff in the Office of the Secretary of Defense, Joint Staff, Air Staff, Office of Science and Technology Policy, Defense Intelligence Agency, National Defense University, and the National Nuclear Security Administration. The other field trip was to Lawrence Livermore National Laboratory in Livermore, Calif. to discuss the technical aspects of nuclear weapons.

Dr. James E. Platte, Dr. Paige Cone, and Dr. Lew Steinhoff were the instructors of this elective and faculty advisors for student research. The research questions for this year's DRTF came from the U.S. Air Force Global Strike Command and the Deputy Chief of Staff for Nuclear Integration and Strategic Stability (Headquarters U.S. Air Force/A10) and were divided into two broad themes. First, how can the United States effectively posture in East Asia for a strategic competition with China? Second, how can the United States prepare for a conflict that potentially escalates to an adversary using a low-yield nuclear weapon?

From those two research themes, the staff selected the best student research papers and placed them into three volumes for publication. Volume 1 is *Extended Deterrence and Strategic Stability in East Asia*. Volume 2 is *Assessing the Influence of Hypersonic Weapons on Deterrence*. Finally, Volume 3 is *Non-U.S. Deterrence Strategies: What Must the United States Be Prepared For?*

CHAPTER 1

Introduction

Nuclear-weapon states around the world continue to develop and advance their nuclear arsenals and strategies. The 2018 *Nuclear Posture Review* succinctly described the strategic environment that the United States faces. "The United States now faces a more diverse and advanced nuclear-threat environment than ever before, with considerable dynamism in potential adversaries' development and deployment programs for nuclear weapons and delivery systems."[1]

In order for the United States to properly prepare for contingencies in this environment, including those that could involve the use of a low-yield nuclear weapon, it is critical to better understand non-U.S. nuclear strategies. U.S. government and military officials must avoid the trap of mirror imaging and not assume that other nuclear-weapon states think and operate like the United States does.

Understanding other nuclear-weapon states' strategies will better enable the United States to both deter adversarial use of nuclear weapons and, if deterrence fails, to fight through a conflict that involves the use of nuclear weapons. As deterrence occurs in the mind of the adversary, having insight into how other nuclear-weapon states view nuclear weapons bolsters the ability of the United States to craft strategies to deter the use of nuclear weapons during peacetime. Even during a conventional conflict, the United States would be able to better control escalation dynamics and deter the introduction of nuclear weapons into that conflict.

Yet, the United States also must be prepared in the event that deterrence fails, and an adversary uses a nuclear weapon. Knowing when, where, and how an adversary may use a nuclear weapon will allow the United States to improve its defenses, recover faster, and continue fighting through an environment affected by the use of a nuclear weapon. American military planners and policymakers cannot afford to be unprepared for adversarial use of nuclear weapons, which requires studying and understanding other nuclear-weapon states' nuclear capabilities and strategies.

With this context in mind, several students from the Academic Year 2019 Deterrence Research Task Force (DRTF) addressed issues related to non-U.S. deterrence strategies. This effort begins in Chapter 2 with Mister Daniel Hooey's study of how Pakistan's pursuit of low-yield nuclear weapons (LYNW) has impacted conceptions of nuclear deterrence and escalation management in the South Asian context. He examined the historical development of nuclear strategy in India and Pakistan and the impact that nuclear weapons have had on India-Pakistan relations. Then, he compared this with the evolving deterrence dynamic under the influence of Pakistan's development of LYNW. Mr. Hooey found that

India maintains a credible second-strike nuclear posture and believes it can deter LYNWs with conventional forces and threat of assured retaliation, but while Pakistan views LYNWs under its full-spectrum deterrence concept, he did not find evidence to believe that Pakistan is purposely lowering the nuclear threshold and pursing nuclear brinkmanship. Still, nuclear weapons are a factor in India-Pakistan conflicts, and the United States must be prepared to play a role in mediating to deescalate conflicts in the future.

In Chapter 3, Col. Anthony T. Shafer, Jr. analyzes the interaction between nuclear deterrence theory and entanglement risks. In this context, entanglement means assigning both conventional and nuclear functions to components of a country's military command and control architecture. Thus, a command and control component could entangle nuclear risks in a conventional conflict. Colonel Shafer steps through the logic of entanglement and finds that regional nuclear powers, with relatively small nuclear arsenals, may purposefully entangle to raise the level of risk to deter conventional attack. American military planners must be aware that some states may seek to entangle as part of their military strategies in order to avoid unintentional escalation in a conflict with a regional nuclear power.

In Chapter 4, Dr. Lyndon "Kyle" McKown examines how adversaries may use nuclear weapons to produce a disabling high-altitude electromagnetic pulse (HEMP) and whether deterrence by denial or deterrence by punishment would be more effective in deterring a HEMP attack. Dr. McKown looks at notional scenarios of HEMP use by three categories of U.S. adversaries: near-peer states, relatively weaker states, and nonstate actors. In general, he concludes that deterrence by denial would be more effective in deterring HEMP attacks across the spectrum of adversaries. Dr. McKown also finds that the United States is inadequately prepared for a HEMP attack and improved resiliency of civilian infrastructure, primarily the power grid, would significantly improve a United States deterrence by denial posture.

Turning to Russian thinking on conflict escalation, Lieutenant Commander Shawn Hughes of the United States Navy analyzes Russian information operations as a potential precursor to military aggression, particularly in Eastern Europe. In Chapter 5, he discusses Russia's long history of using information operations, with a regional focus on Russia's periphery. Also, Commander Hughes studies Russia's use of information operations in Georgia, Ukraine, and Estonia. He finds that Russian conventional operations follow information operations, except against NATO-aligned states. Therefore, Russian information operations must be identified early so planners can devise countermeasures and prevent escalation to kinetic military aggression.

Finally, Chapter 6 concludes this volume with some final thoughts and recommendations for further research.

Chapter 1 Note

1. Office of the Secretary of Defense, *Nuclear Posture Review* (Washington, D.C.: Department of Defense, February 2018), p. 5. Accessed at https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

CHAPTER 2

Pakistan's Low-Yield in the Field: Diligent Deterrence or De-escalation Debacle

Mr. Daniel Hooey, DIA/USCENTCOM

Having engaged in three wars and numerous border crises, the potential for future conflict between Pakistan and India remains high. However, the prospects of escalation towards a nuclear exchange are a subject of rich debate among Western and South Asian scholars.[1] While the nuclear exploits of both countries trace back to the 1960s, the research for this study will focus on developments observed since declared nuclearization in 1998 – most notably Pakistan's ongoing pursuit of low-yield nuclear weapons (LYNWs).[2] The nuclear beginnings of both states occurred clandestinely, outside the recognized "nuclear norms" of the five established nuclear-armed states.[3] These nuclear programs, born of failed nonproliferation efforts and viewed with ire by the international community, drew sanctions and diplomatic pressure to sign nuclear treaties to conform with global efforts of inventory reductions, nuclear test bans, and disarmament. Having refused these overtures, both India and Pakistan continued to develop their nuclear programs, albeit towards seemingly different ends.

India has largely modeled its nuclear doctrine and behaviors after the established nuclear states, while Pakistan has avoided the restraints of nuclear no first use and seeks to proactively leverage the regional deterrence paradigm to its full advantage. Pakistan's nuclear intentions have evolved into its burgeoning concept of "full-spectrum deterrence," which seeks to lower the nuclear threshold to include low-yield nuclear options against all threats ranging from tactical to strategic.[4] Pakistan's rationale for such a strategy is similar to that of the United States in Europe during the Cold War where LYNWs were used to offset Soviet conventional superiority. Under these conditions, both the United States and the Soviet Union clearly understood that any conventional conflict in Europe would carry nuclear potential, a distinction that may not necessarily hold true in the South Asian context.

This paper employs a comprehensive approach to evaluate two hypotheses using a body of Western and South Asian scholarly works that specifically pertain to the Indo-Pakistan nuclear paradigm. Given the preponderance of comparisons between Pakistan's pursuit of LYNWs to the United States employment of these systems in Europe, this research begins with a comparison of these case studies. The paper then outlines the respective nuclear doctrines and postures of both Pakistan and India and subsequently explores Pakistan's introduction of LYNWs and their impact on South Asian deterrence. Following this is evaluation and testing of the two hypotheses, along with an assessment of the potential for a nuclear conflict in South Asia. The research paper culminates with sections exploring implications and opportunities.

The research specifically examines the question of how has Pakistan's pursuit of LYNWs impacted both Indian and Pakistani conceptions of deterrence and escalation management. Out of this question comes two independent hypotheses: The first hypothesis (*H1*) asserts India will seek to maintain a credible second-strike nuclear posture and believes it can deter Pakistan's LYNWs with conventional forces and the threat of assured retaliation. The second hypothesis (*H2*) asserts Pakistan views LYNWs under full-spectrum deterrence as a mechanism to lower the nuclear threshold as an instrument of brinksmanship. This research does not specifically assume or imply that a nuclear conflict between the two states will ever occur, but seeks to evaluate how the introduction of LYNWs into the region will alter regional deterrence postures and associated implications on international mediation.

Comparative U.S. Lessons on Low-Yield Weapons During the Cold War

The preponderance of Western and South Asian scholars believe Pakistan's move toward LYNWs is predicated upon observations of the U.S. employment of these systems in Eastern Europe during the Cold War.[5] The rationale of the United States for the employment of LYNWs was to deliberately lower the nuclear threshold to deter the possibility of Soviet aggression from adjacent Warsaw Pact nations.[6] The United States elected to employ LYNWs as standoff systems to circumvent the need to commit, and inherently sustain, the enormous amount of military resources that would be required to offset such conventional asymmetry. LYNWs in this context, were a cost-effective alternative that successfully deterred Soviet aggression against NATO allies in Europe. However, these efforts carried enormous risks.[7] The U.S. military developed and fully integrated LYNWs into its arsenal before applying any meaningful consideration to the doctrine or practical employment of such systems.[8]

For LYNWs to be successful as a stand-off weapon, nuclear command, control, and communications (NC3) must be pre-delegated to battlefield commanders, thus making them warfighting weapons rather than strategic ones. Pre-delegation of authority puts the onus of nuclear decision making in the hands of field grade military officers on the forward edges of the battlefield. LYNWs required forward deployment, due to their limited range, which invited the

conditions for a "use it or lose it" scenario. These same field grade officers could have quickly encountered such a scenario had Soviet forces elected to advance even a short distance, a rather considerable deterrence gamble. Western nuclear scholars such as Eric Schlosser observe pre-delegated NC3 structures also introduce the potential for unauthorized or accidental use, a real possibility given the number of accidents involving nuclear weapons that occurred during sustained periods of heightened nuclear alert throughout the Cold War.[9]

Another LYNW dilemma the United States never resolved during this period was that survivability in a nuclear environment requires a dispersion of assets. However, winning conventional ground conflicts invokes principles of mass and concentration of forces. The actual use of LYNWs would further preclude force concentration as the fallout would restrict maneuver and reduce, or eliminate, mobility corridors.[10] In essence, LYNWs proved ineffective at enhancing conventional deterrence credibility as they prohibit the employment of corresponding ground forces in a combat-effective manner.[11] Failure to resolve this issue eventually led the U.S. military to deduce that these weapons would merely be employed in a manner that gave pause to the Soviets by confronting them with prospects of escalation while simultaneously leveraging the threat of an all-out nuclear war.[12] As mentioned previously, both sides clearly acknowledged that any conventional conflict carried nuclear potential and the strategic culture of the time considered LYNWs as another variation of warfighting weapons in this context. Eventually the United States and Soviet Union acknowledged the dangers associated with such strategies and removed LYNWs from Europe in 1987 upon signing the Intermediate-Range Nuclear Forces Treaty (INF).[13]

Pakistan faces similar challenges as it faces a conventionally superior Indian adversary. Having already lost two conventional wars, and endured numerous border crises with India, Pakistan considers its nuclear arsenal the guarantor of its national sovereignty and a key instrument of state survival. Conventional military asymmetry, and an inability to compete with India economically, render Pakistan incapable of addressing the widening military gap despite attempts to modernize and expand its military capabilities.[14] As such, it is not surprising that Pakistan would turn to its nuclear arsenal, much like the United States did in Europe, for solutions to its lack of conventional parity. While contemporary nuclear scholarship and the current strategic culture clearly delineate between conventional and nuclear forms of conflict, Cold War nuclear theory and military strategic culture did not make such distinctions and Pakistan's consumption of literature from this era could lead Islamabad to more precarious conclusions.

A robust study by American scholars compared Pakistan's LYNW pursuits to those of the United States during the Cold War and revealed striking similarities in Islamabad's approaches and rationale for the employment of LYNWs. The study showed that Pakistani nuclear scholarship focused almost exclusively on the traditional works of U.S. nuclear scholars such as Thomas Schelling, Herman Kahn, Bernard Brodie, etc. The conclusions drawn from these works were limited to perceived successes of Cold War LYNW deterrence models.[15] This problem is exacerbated by the Pakistani military's compartmentalization of nuclear matters as evidenced when Sannia Abdullah noted, "Stringent control on nuclear policy and

debate deprives academics, journalists and other members of the civil society to give policy input on nuclear issues."[16] The study also noted that Pakistani scholars and military professionals tend to lack an understanding, or ignore altogether, the risks, failures, and lessons learned from the U.S. employment of LYNWs in Europe.[17] As such, Islamabad has narrowly focused on the deterrence benefits of LYNWs, but has dismissed the associated risks and consequences these nuclear postures entail.[18]

Pakistan's Nuclear Doctrine and Posture

Nuclear Doctrine

Pakistan views its nuclear arsenal as the ultimate guarantor of its sovereignty and national survival against India. Its nuclear doctrine seeks not only to deter Indian nuclear use, but also the prospects of conventional aggression. Though Pakistan has not officially declared a nuclear doctrine, instead invoking principles of selective ambiguity, Islamabad's policies and actions since 1998 have revealed its core tenets.[19] South Asian scholars such as Gurmeet Kanwal posit, "Ambiguity has been used as an offset for conventional inferiority with the belief that control over escalation is possible."[20] Pakistan's nuclear doctrine encompasses four primary principles: Indo-centric minimum nuclear deterrence; massive retaliation (although its limited arsenal may not lend itself to such); nuclear first-use; and strategies that emphasize countervalue nuclear targeting.[21] While Pakistan's nuclear posture has shifted in response to regional threat perceptions, there has been little observable change to its salient doctrinal features.

Pakistan operates under a true nuclear dyad, which allows Islamabad to focus its entire nuclear contingent against a singular adversary. The associated regional dynamics pose unique challenges, given the geographical contiguity between the two countries. The associated lack of geographic depth or standoff inherently alters the nuclear dynamics between the countries and complicates nuclear employment and respective doctrinal capabilities.[22] While Pakistan claims a policy of minimum deterrence, this is more likely out of necessity than choice. As opposed to India, which deliberately chooses to limit the size of its nuclear arsenal, Pakistan is forced to do so given its budgetary and fissile material production constraints that have infringed on its nuclear ambitions.[23]

Massive retaliation is a key facet of Pakistan's nuclear doctrine, although its limited arsenal probably lends itself more towards assured retaliation by Western standards. South Asian scholars believe this is driven by two factors: the need to deter a potential Indian preemptive strike against its nuclear arsenal and to offset its conventional inferiority.[24] Pakistan's progression towards a nuclear triad, and concerns over India's burgeoning ballistic missile defenses (BMD), are testaments to Islamabad's doubts in the credibility of its second-strike capabilities and will serve as a justification for a larger (and more diverse) arsenal.[25] Experts believe Pakistan is rapidly expanding its arsenal, which could put it on pace to surpass Britain and France in terms of its nuclear inventory. However, Pakistan could

exhaust its sources of uranium ore by 2020, putting it at an upper limit of around 250 strategic weapons.[26]

Pakistan's selection of nuclear first-use was an obvious choice given its lack of conventional parity with India, which has required Islamabad to threaten the use of its full nuclear complement to buttress its nuclear credibility. It is important to note that this inherently makes Pakistan more prone to consider the use of nuclear weapons as a warfighting capability, which in part explains Islamabad's pursuit of LYNWs. The fact that many of Pakistan's key cities are within close striking distance of the border also heightens Pakistani perceptions of strategic vulnerability, which makes the prospects of first-use more appealing as it offers more flexibility. Enduring concerns over the survivability of its second-strike capabilities and more recently, India's advancements in missile technology to include hypersonic variations of its *Brahmos II*, continue to make nuclear first-use the most viable option.[27] The "use it or lose it" dilemma faced by countries that typically adopt first-use postures will similarly challenge Pakistan as LYNWs will be subject to these issues.[28]

There are several factors that shape Pakistan's doctrine regarding countervalue targeting. The relatively small size of Pakistan's arsenal makes it important to maximize punishment on New Delhi, which is likely why Islamabad (perhaps mistakenly) terms it a policy of maximum retaliation. Neither India nor Pakistan possess a sufficient arsenal to achieve the Cold War measure of mutually assured destruction (MAD), but both possess the ability to sufficiently destroy large swathes of each other's territory. However, India's strategic depth, combined with the lack of reach of Pakistan's weapons (although this is improving), would render efforts to preemptively attack Indian strategic assets ineffective, thus giving Pakistan little hope of achieving a successful decapitation while simultaneously subjecting it to assured retaliation from India. Indian population and industrial centers are within striking distance of Pakistani nuclear weapons making them lucrative targets that are easier to engage.[29]

Nuclear Posture

The most substantive analysis of South Asian nuclear postures can be derived from the extensive analysis of Vipin Narang. Narang asserts that Pakistan started with a more stable catalytic posture that relies upon the intervention of a third-party patron, which at that time was the United States.[30] However, the rather tumultuous nature of U.S.-Pakistani relations over the years that has been fraught with mutual distrust and perceptions of abandonment by the United States, led to an eventual shift towards a more dangerous and unstable asymmetric escalation posture.[31] The exact state of Pakistan's nuclear readiness is unknown. However, Islamabad claims it maintains a low state of readiness with its warheads stored at dispersed locations in a disassembled state.[32] While Pakistan's strategic systems are not believed to be stored in a ready state, this may not apply to its developing LYNWs. The air launched cruise missile (ALCM), sea launched cruise missile (SLCM), and ground launched cruise missile (GLCM) variations of Pakistan's low-yield systems are believed to be produced and stored in a fully-assembled state.[33]

Pakistan claims it has no plans to proactively disperse its low-yield systems, which is not surprising as doing so would invite preemptive or preventative strikes by India. However, Pakistan warns these systems are stored in a manner that allows them to be deployed quickly during a crisis, alluding to a period of hours, not days *(See Table 1*).[34]

Table 1. Pakistan's Nuclear Forces[35]

Pakistan's Nuclear Forces as of 2018					
Type	**Number of Launchers**	**Year Deployed**	**Range (km)**	**Warhead x Yield (kt)**	**Number of Warheads**
F-16 A/B (aircraft)	~24	1998	1600	1 x bomb	~24
Mirage III/V (aircraft)	~12	1998	2100	1 x bomb	~12
Abdali / Hatf-2 (land-based ballistic missile)	10	2015	200	1 x 5-12	10
Ghaznavi / Hatf-3 (land-based ballistic missile)	~16	2004	300	1 x 5-12	~16
Shaheen-1 / Hatf-4 (land-based ballistic missile)	~16	2003	750	1 x 5-12	~16
Shaheen 1A / Hatf-4 (land-based ballistic missile)	N/A	2018	900	1 x 5-12	N/A
Shaheen 2 / Hatf-6 (land-based ballistic missile)	~12	2014	1500	1 x 10-40	~12
Shaheen 3 / Hatf-6 (land-based ballistic missile)	N/A	2018*	2750	1 x 10-40	N/A
Ghauri / Hatf-5 (land-based ballistic missile)	~24	2003	1250	1 x 10-40	~24
NASR / Hatf-9 (land-based ballistic missile)	~24	2013	60-70	1 x 5-12	~24
Ababeel (land-based ballistic missile)	N/A	N/A	2200	MIRV	N/A
Babur / Hatf-7 (GLCM)	N/A	2014	350	1 x 5-12	~12
Babur 2/1 (GLCM)	N/A	N/A	700	1 x 5-12	N/A
Ra'ad (ALCM)	N/A	2017	350	1 x 5-12	N/A
Ra'ad 2 (ALCM)	N/A	2018*	>350	1 x 5-12	N/A
Babur 3 (SLCM)	N/A	N/A	450	1 x 5-12	N/A
				Total	~140-150**
* Estimated Deployment Timeframe			**Total Numbers are Approximate		

India's Nuclear Doctrine and Posture

> *"If New Delhi goes up in a mushroom cloud, a certain theater commander will go to a safe, open his book, and begin reading on page one, paragraph one, and will act step by step on the basis of what he reads."* – Vipin Narang

Nuclear Doctrine

Ashley Tellis, a scholar and a recognized authority on Indian nuclear doctrine, posits, "Any discussion of India's nuclear doctrine and force posture is by definition fraught with uncertainty" and something that could take decades to sort out.[36] Tellis notes that doctrine progresses at the pace of technological advancement, which is in itself unpredictable, along with other conditions or stimuli that may arise that prompt rapid change. Such may be the case with Pakistan's introduction of LYNWs.[37] India released its "Draft Report of the National Security Advisory Board on Indian Nuclear Doctrine" on Aug. 17, 1999, which represents the most comprehensive document on Indian nuclear doctrine that New Delhi has ever produced.[38] Many experts claim that there has been little change to the core tenets of the doctrine since the draft was released. However, Tellis cautions the draft was written as recommendations that do not necessarily reflect settled policy.[39] From its inception, the policy was not only provocative for Pakistan and China, but also highly contested internally.[40]

A largely unchanged version of the doctrine was released in 2003 that included the key concepts of no first use, minimum credible deterrence, and assured retaliation. According to Vipin Narang, the overriding intent of India's doctrine is to, "deter the use and threat of use of nuclear weapons by maintaining an adequate retaliatory capability should deterrence fail."[41] Many scholars, including Narang, believe this posture suggests India will absorb the first nuclear blow and will invoke its doctrine of assured retaliation to authorize a strategic nuclear response.[42] It is this point that draws contention among contemporary critics of no first use who assert this weakens India's deterrence credibility. However, Tellis notes that this concept is, "remarkably pervasive in Indian strategic thought," which may explain why this policy has endured despite prolonged disputation.[43] India's doctrine also calls for minimum credible deterrence, seeking to achieve deterrent effects with a limited arsenal.[44] However, there are indications that India, like Pakistan, considers the size of its arsenal to be a fluid concept that must be responsive to the actions of its adversaries.[45] As Pakistan and China expand and diversify their respective arsenals, it is only reasonable to assume that India will also do so in kind to maintain deterrence credibility.

Assured retaliation is a significant, although also highly contested, aspect of India's nuclear doctrine. India does not consider nuclear weapons as warfighting options, but as instruments of punishment to inflict maximum damage against an adversary should deterrence fail.[46] Tellis further qualifies this concept as "delayed, but assured retaliation." As India is postured for punitive operations, it therefore must consider that the ability to retaliate is more important than the timing of the

response.[47] While there is no specified timeline for a nuclear response, it must be assumed that India will be required to calculate its reaction, ready the required delivery vehicles and warheads, and commence the NC3 authorization process. While there are recent indications that India has enacted measures to reduce nuclear response times, there is a reasonable expectation for delay due to New Delhi's highly centralized NC3 structure. The final facet of Indian nuclear doctrine pertains to strategic nuclear targeting. Given that Indian doctrine restricts nuclear use to punishment, Tellis (and others) assess that nuclear weapons will be directed against primarily countervalue (civilian) targets.[48] This is further evidenced by India's propensity to use these weapons towards achieving political ends instead of achieving any sort of military objectives on the battlefield.[49] As such, Tellis concludes, "India is almost certain to settle for countervalue targeting and, by implication, seek to service a nuclear strategy centered on some kind of mutual assured vulnerability."[50]

Nuclear Posture

Narang offers useful insights into India's nuclear posture noting three specific pillars of India's nuclear policy including: no first use, assured massive retaliation, and under "no condition will the weapons be conventionalized."[51] Under these pretenses, Narang's model categorizes New Delhi's nuclear posture as one of assured retaliation. While India lacks the strategic reach to target the entirety of Chinese or Pakistani territory, it retains the ability to inflict substantial damage against either state, which substantiates its deterrence credibility. Its technological advancements are quickly narrowing this gap.[52] Despite some indications of internal debate, there are no indications that India has officially altered any facets of its existing nuclear posture in response to Pakistan's fielding of LYNWs *(See Table 2).*

Table 2 (India's Nuclear Forces)[53]

India's Nuclear Forces as of 2017					
Type	**Number of Launchers**	**Year Deployed**	**Range (km)**	**Warhead x Yield (kt)**	**Number of Warheads**
Vajra – Mirage 200H (aircraft)	~16	1985	1850	1 x bomb	~16
Shamsher – Jaguar IS/IB (aircraft)	~32	1981	1600	1 x bomb	~32
Prithvi-2 (land-based ballistic missile)	~24	2003	350	1 x 12	~24
Agni-1 (land-based ballistic missile)	~20	2007	700+	1 x 40	~20
Agni-2 (land-based ballistic missile)	~16	2011	2000+	1 x 40	~16
Agni-3 (land-based ballistic missile)	~8	~2014	3200+	1 x 40	~8
Agni-4 (land-based ballistic missile)	N/A	2018*	3500+	1 x 40	N/A
Agni-5 (land-based ballistic missile)	N/A	2020*	5200+	1 x 40	N/A
Dhanush (sea-based ballistic missile)	2	2013	400	1 x 12	2
K-15 (sea-based ballistic missile)	12	2017	700	1 x 12	12
K-4 (sea-based ballistic missile)	N/A	UNK	~3000	1 x UNK	N/A
				Total	~118**
* Estimated Deployment Timeframe				**Total Numbers are Approximate	

Pakistan's Introduction of Low-yield Nuclear Weapons to the Deterrence Paradigm

LYNWs, in nearly every facet of employment, tend to complicate traditional concepts of deterrence and necessitate considerations of limited nuclear war. American nuclear scholars such as Jeffrey Larsen and Kerry Kartchner have assessed and evaluated the many challenges associated with the possibility of limited nuclear war – a prospect so dangerous that the United States and the Soviet Union bilaterally agreed to abandon these practices in Europe. As Lawrence Freedman famously wrote, "It takes two to keep a war limited," a lesson that no doubt applies to the South Asian dynamic, perhaps in more striking ways. At face value, the animosity between the two countries is not so different from other adversarial relationships in the international system, but what makes this relationship different is the fact that all major crises since nuclearization have required a degree of international mediation assistance.[54] The fact that these countries do not effectively engage on a state-to-state level, even during periods of enormous bilateral tension, creates an obvious deterrence issue, which decreases the probability of effective communication of nuclear signaling or de-escalation measures (i.e. off ramps) during the progression of a crisis.[55] These challenges are exacerbated by a heightened potential for confirmation bias during a crisis – given the inability of both sides to objectively detect, process, and validate the intentions of the other. A lowered nuclear threshold and the decentralized nuclear authority

structure inherent to LYNWs will inevitably reduce decision space for senior leaders on both sides, which could make this a recipe for disaster.

Driven by its development and ongoing integration of LYNWs, Pakistan has adopted its doctrine of full-spectrum deterrence, which seeks to lower the nuclear threshold to provide Islamabad the flexibility to contend with even conventional threats from India. Inderjit Panjrath notes four central themes that are apparent in Pakistani official statements about full-spectrum deterrence. First, LYNWs were a response to India's Cold Start doctrine that seeks to rapidly conduct numerous limited military penetrations to secure Pakistani territory while remaining under the nuclear threshold.[56] Second, Pakistan acknowledges that any battlefield use would have strategic consequences. Third, full-spectrum deterrence is not a war-fighting strategy, but rather a strategy to deter limited conventional war below Pakistan's existing threshold for nuclear use. Fourth, Pakistan will maintain centralized command and control of LYNWs in the same manner as its strategic arsenal.[57]

While superficially reassuring, these endeavors tend to alter the deterrence paradigm between the affected states as observed during the similar introduction of LYNWs in Europe during the Cold War. As Dave Smith surmised, "Pakistan's decision to embrace tactical nuclear weaponry will ultimately require it to deal with the doctrinal implications, increased security and command and control requirements, and the potentially destabilizing implications of deploying such weapons."[58]

Pakistan's development of a low-yield triad to increase the credibility of its second-strike capability will further disrupt the deterrence paradigm and will hasten reciprocal Indian efforts to acquire comparable capabilities to defeat Pakistan's systems. These developments were probably a component of India's continued pursuit of a viable BMD system, which threatens the credibility of Pakistan's strategic delivery vehicles. Such developments will inevitably invoke further South Asian arms races in the future. However, India's economic and already significant qualitative and quantitative military advantages, will increasingly widen the gap and stimulate further Pakistani strategic paranoia. This dichotomy is unsustainable for Islamabad, whose failing economy will continue to constrain its military development and nuclear ambitions. Unlike India, whose conditional Nuclear Suppliers Group (NSG) status grants New Delhi the ability to purchase nuclear materials, Pakistan's inability to secure additional fissile material from external sources will significantly hamper its future efforts.

Another change to the deterrence paradigm stems from the potential for dispersal and the NC3 structure for LYNWs. There are indications that Pakistan actively employs denial and deception measures such as dummies and decoys. Pakistan routinely shuffles its strategic nuclear assets among a dozen or more secret bunkers in addition to several other phony locations.[59] There are also suspicions of various dummy sites in an elaborate tunnel network to optimize the prospects of survivability.[60] The intermingling of conventional and nuclear tipped systems, coupled with elaborate denial and deception mechanisms, could inadvertently provoke an Indian preventative strike if these systems were dispersed during a crisis regardless of the type of munition used.[61]

The other issue concerns the NC3 of LYNWs as Inderjit Panjrath observed, "Pre-delegation to field commanders was an integral part of credible deterrence through TNWs [tactical nuclear weapons]."[62] American scholars reverberate these concerns as they identify Pakistan as one of the few nuclear states that has adopted such a structure.[63] Delegative NC3 postures do provide advantages as they diversify launch authority, which negates the prospects of a decapitation strike and allows for rapid assembly, deployment, and delivery of nuclear weapons during crisis situations while providing few physical barriers to their release.[64] The dangers of this posture were never solved by the United States in Europe and invite a high potential for miscalculation, nuclear accidents, or inadvertent and/or unauthorized use.

India's Reaction to Full-Spectrum Deterrence

The various works of South Asian and Western scholars suggest India may be struggling to cope with the prospects of full-spectrum deterrence. This is not surprising as these struggles are reminiscent of the very same deterrence dilemmas experienced by both the United States and the Soviet Union regarding LYNWs. Indian discord over full-spectrum deterrence is confined to two primary spheres of thought. Nuclear pessimists advocate for an alteration of India's current doctrine to address the prospects of full-spectrum deterrence. Nuclear optimists believe full-spectrum deterrence can be mitigated through existing means without the need to alter or adapt existing doctrine. Each side presents a relatively strong case to substantiate its respective claims. It is also important to note there are areas of convergence between the two camps – all of which are explored more thoroughly in the rest of this section.

Nuclear pessimists contest that India's doctrinal concepts of no first use and assured retaliation make New Delhi vulnerable to acts of Pakistani provocation, essentially rendering India strategically paralyzed.[65] While India's current doctrine of assured retaliation reserves the right to use nuclear weapons if any weapons of mass destruction (WMD) are used on any Indian forces anywhere, pessimists feel this may be insufficient to deal with full-spectrum deterrence.[66] Pessimists have also called for the Indian military to develop a reciprocal low-yield capability to allow for a proportional response should Pakistan detonate LYNWs during a future crisis or conflict.[67] There has also been significant emphasis on developing a robust BMD capability that is seemingly based on the Israeli Iron Dome model. Several of the components of the system such as the Green Pine radar and associated interceptor missile systems have already been acquired from Tel Aviv.[68] While the Indian political community writ large considers India's nuclear arsenal purely strategic, there are indications New Delhi may be trending towards a higher state of readiness. Vipin Narang notes India may be pursuing avenues such as "canisterization," which is a method of hermetically sealing and storing a fully mated warhead to reduce preparation timelines during future crises.[69]

Nuclear optimists tend to downplay the threat of full-spectrum deterrence, instead highlighting the benefits of adhering to India's existing doctrine. Nuclear optimists argue that India capitalizes on the benefits of recognition as a responsible

actor within the international community by ignoring Pakistan's provocative actions. These efforts, in no small part, helped secure their conditional entry into the NSG and may outweigh the risks of electing not to respond.[70] Extensive studies have also revealed the ineffectiveness of LYNWs against advancing armor columns, which is what many Indian military experts assess to be the primary target of Pakistan's LYNWs.[71] It would take hundreds of these systems to destroy a single armored division, which would quickly exhaust Pakistan's LYNW inventory and inevitably incite an Indian reprisal in the form of a full-scale nuclear retaliation with its strategic assets.[72] In addition, LYNWs would place high demands on Pakistan's existing plutonium stocks as these systems require a significant amount of fissile material to produce and would be capable of achieving only marginal effects on the battlefield.[73] It is these considerations that prompt some optimists to categorize these systems as "showcase weapons" instead of viable warfighting systems.[74] Optimists also posit that regardless of the promises of full-spectrum deterrence, there is still room under the nuclear umbrella for conventional military action. The "surgical strikes" conducted by Indian special forces in September 2016 in response to the Uri terrorist attacks are cited as evidence of this – full-spectrum deterrence had already been implemented at this time.[75]

Both sides also agree on several core issues including actively exploring ways to mitigate Pakistan's ability to export terrorism under the umbrella of nuclear blackmail.[76] Both camps also seem to agree that the political space for Indian restraint in the face of continued terrorist attacks emanating from Pakistani soil is rapidly diminishing – a point that also concerns Western scholars.[77] Hardliners within India's current Modi government have popularized the prospects of assuming a firmer stance regarding Pakistan, which may progressively drive the political establishment towards more provocative responses in the future to preserve political capital.[78] Another area of convergence involves addressing issues with Pakistan in a manner that preserves India's positive image in the international community.[79]

Low-Yield Rationale: Pakistan Coping With Asymmetry or Strategic Brinksmanship

> *"A nuclear state can coerce its opponent by taking dangerous escalatory actions that increase the risk of an unintended disaster. Although both sides understand that the other would not rationally start a nuclear war, the possibility of accidental nuclear escalation can turn seemingly incredible threats into credible ones."*
>
> – Todd Sechser and Matthew Fuhrmann

This section evaluates the two research hypotheses pertaining to the insertion of LYNWs into the South Asian nuclear context. The first hypothesis (*H1*) asserts that India will seek to maintain a credible second-strike nuclear posture and believes it can deter LYNWs with conventional forces and the threat of assured retaliation. The second hypothesis (*H2*) asserts Pakistan views LYNWs under its policy of full-spectrum deterrence as a mechanism to lower the nuclear threshold

as an instrument of brinksmanship. The remainder of this section tests each of these hypotheses using the entirety of the research presented and evaluates the supporting evidence for *H1*, the evidence that refutes *H1*, the evidence that supports *H2*, and the evidence that refutes *H2*. The section concludes with a summary of the findings.

Hypothesis 1

H1 attempts to explain how India would cope with the introduction of LYNWs as New Delhi must contend with two nuclear-armed adversaries in both Pakistan and China. Despite recent debate over some facets of India's doctrine, no significant changes have been made to its core tenets since its drafting in 1999 regardless of Pakistan's intent to field LYNWs. Most experts seem satisfied with the guarantees of India's existing doctrine of assured retaliation, which calls for a strategic response to the use of WMD against Indian forces operating anywhere. While there are scholars who advocate for India to develop a reciprocal low-yield capability, there is no evidence that India has developed a low-yield equivalent or even intends to do so. The preponderance of Western and South Asian scholars agree that LYNWs do not pose a significant threat to advancing armor forces and do not significantly improve deterrence credibility based upon empirical evidence from the experience of the United States in Europe and assessed conditions in South Asia.

Indian and Western scholars surmise that, like NATO, these systems are not meant for battlefield use and are more of a "showcase weapon" with limited range and yield.[80] Indian and Western scholars also agree that the tremendous fissile material commitments for these weapons make them unlikely to be widely fielded and if they were proactively dispersed, would be easy targets of Indian preemptive strikes.[81] Indian scholars such as Panjrath also believe there is still room for conventional actions under the nuclear umbrella citing the "surgical strikes" conducted after Uri.[82] There is also evidence that India is continuing to improve its second-strike credibility through the acquisition of nuclear submarines and exploration of advanced delivery vehicle technologies.[83]

While a large body of evidence supports *H1*, there is also some contradictory evidence that counters this claim. Both Western and South Asian scholars assess that Indian tolerance for continued attacks by Pakistani terrorists is diminishing, and with it, prospects of strategic restraint. While India has elected to curb its present response to LYNWs, this sentiment may not prevail in the long term, particularly given growing concerns of nuclear blackmail. Hardliners in the existing Modi government have popularized a hard stance, a trend that is expected to continue as future politicians campaign for office, which may lead to future changes to India's nuclear posture. There is a body of nuclear pessimists who are calling for changes to the existing nuclear doctrine, most notably its policies of no first use and assured retaliation. However, these calls do not appear to reflect the sentiments of the civilian government, which would be the only officials empowered to alter the doctrine.[84] While this has not yet prompted changes, additional crises or provocative actions by Pakistan could give these arguments more traction to incite future change.

Hypothesis 2

H2 seeks to explain Pakistan's rationale and end state for the development of nuclear weapons. There is strong evidence to support the first portion of *H2*, which asserts full-spectrum deterrence seeks to lower the nuclear threshold. Pakistani officials claim this was exactly what these systems were intended to do. Western and South Asian scholars almost unanimously agree that Pakistan is following the model set forth by the United States using LYNWs as a means of lowering the nuclear threshold. There is also evidence that indicates these weapons may not be intended for battlefield use, but as standoff weapons like those deployed by the United States in Europe. There is no evidence that refutes the use of LYNWs to lower the nuclear threshold. However, there are significant challenges associated with *H2*.

The difficulty with proving or disproving *H2* relates to the second portion of the hypothesis that deals with nuclear brinksmanship. While the introduction of LYNWs carries numerous inherent risks, and a possibility of being used for brinksmanship, there is no evidence to suggest that Pakistan has leveraged them, or even intends to leverage them, for deliberate escalatory actions. Pakistan certainly realizes that provoking an Indian strategic nuclear response would invoke destruction of the Pakistani state. However, this realization may not stop Islamabad from manipulating the conditions during an escalation in hopes of obtaining concessions from India. While LYNWs may not be deliberately intended to create the conditions for brinkmanship, there may be opportunities for such exploitation to occur as a crisis evolves. Indian scholars openly accuse Pakistan of shielding terrorism with nuclear blackmail, and while perhaps not entirely untrue, there is little more than Indian accusations to substantiate this claim. The preponderance of evidence suggests that Pakistan, concerned over the reduced credibility of its deterrence against a conventionally superior adversary, has simply leveraged its most powerful instrument of war to address perceived conventional gaps. While it does so in a conceivably dangerous manner, this is not evidence of brinksmanship.

Assessment

In sum, research validates *H1* as the bulk of the evidence suggests that India has not deviated from its existing strategies in response to LYNWs. There could be a variety of drivers for this, but there seems to be a prevailing sentiment that India has much more to lose with regards to international credibility by responding in a manner that would be perceived as irrational. There are no indications that deterrence considerations concerning China have substantively impacted India's calculus with regards to LYNWs. New Delhi seems comfortable with its existing deterrence posture, aided by natural defensive terrain advantages along its northern border.[85] Per the available evidence, the results of *H2* are inconclusive. While the aspects of lowering the nuclear threshold are not in question, the subsequent prospects of nuclear brinksmanship have not been definitively proven. There is little evidence to suggest Pakistan is deliberately engaging in nuclear

brinksmanship. However, there is nothing saying that it has not, or will not, do so in the future.

Assessing the Potential for the Great Nuclear Misadventure

> *"In western capitals, there's particular concern that the introduction of tactical nuclear weapons (TNW) lowers the nuclear-use threshold, making nuclear war more likely. According to one recent study, such a war in South Asia could kill 20 million people in the first week then put up to two billion people at risk of famine globally*."
>
> – Mark Fitzpatrick

While it is easy to dismiss the enduring problems between India and Pakistan as merely a regional issue that can be worked out bilaterally, the impacts of even a limited nuclear conflict carry grave consequences that extend far beyond the region. American scholars offer a grim and sobering view of what LYNWs could mean in the South Asian context. The United States previously reached similar conclusions about LYNWs in Europe as initial war games and exercises in the 1950s revealed. "In only nine days of simulated nuclear combat, West Germany was judged to have suffered three times the civilian casualties of World War II."[86] Historic assessments have shown the consequences of even the most limited nuclear exchange are far reaching and produce a strategic effect regardless of yield. The integration of LYNWs introduces additional factors that must be carefully considered, such as increased potential for miscalculation, nuclear accidents, and/or unauthorized use, and impacts to the intervention calculus. This will be explored in more detail in the paragraphs that follow.

One of the more difficult challenges of LYNWs is their inherently destabilizing nature, exacerbated by Pakistan's propensity towards nuclear ambiguity that in turn creates an environment rife with miscalculation potential. While Pakistan and India have successfully maneuvered their way through various crises and international incidents over the years using a bilaterally understood framework of escalation management, the introduction of LYNWs may have a significant impact on the calculations of both countries. Given that Pakistan's ground-based LYNWs are considered dual-use systems with conventional and nuclear-tipped munitions, even a benign deployment of high-explosive (HE) equipped systems could cause a significant overreaction by India who may misperceive such systems as an escalation to a nuclear level.[87] Pakistan could also elect to intentionally deploy conventional low-yield systems (real or decoy) to attempt to coerce India to stand down during a period of heightened tensions – using these systems as a dangerous instrument of battlefield signaling. Another key facet of miscalculation involves target selection. As mentioned previously, Indian scholars have wrestled internally with the doctrinal prospects of assured retaliation, which do not adequately address the threat of LYNWs.[88] As such, questions arise as to what response options India would contemplate in the event Pakistan actually

employed such systems during a crisis.[89] Will it matter if Pakistan uses LYNWs against advancing Indian forces on its own soil? Does countervalue (civilian) targeting versus counterforce (military) make a difference in the Indian calculus? Given India does not possess a LYNW equivalent, does proportionality matter enough to prevent them from using a strategic weapon in response? The fact that New Delhi itself does not have clear answers to these difficult questions should theoretically give Pakistan pause to carefully consider how it employs such assets. However, this does not appear to be the case.[90]

The second factor involves the potential for accidental or unauthorized use, which was also a significant concern for the United States during Cold War employment of LYNWs. American scholars like Eric Schlosser conclude that sustaining a high level of nuclear alert creates the conditions for an "always/never" dilemma. Under these conditions, nuclear weapons are expected to always work when called upon and never fail. Western scholars have expressed serious doubt regarding the safety measures of low-yield delivery vehicles as such systems are expected to be made field expedient for rapid use on order. These circumstances favor the "always" to the detriment of the "never."[91] There is also a question as to whether Pakistan's LYNWs have been subjected to the same level of safety scrutiny as its strategic systems, namely weapons that are one-point safe.[92] The absence of strong safety controls and centralized authorization mechanisms during crises not only makes the weapons less safe (accidental use), but these same deficiencies also make them vulnerable to unauthorized use.[93] Pakistan has a demonstrated vulnerability to insider attacks as evidenced by the assassination of the Punjab governor by members of his own security detail, various unsuccessful assassination attempts against President Pervez Musharraf, and numerous attacks against Pakistani military installations.[94] While there are stringent personnel evaluation controls in place to actively monitor members of Pakistan's nuclear community, it is unknown to what degree these measures are applied to crews operating the various components of Pakistan's LYNW arsenal. The delegative nature of the NC3 authority for LYNWs place high decision capital on relatively junior military officers in the field, which could create the conditions of "rogue majors" to take actions into their own hands without authorization.[95] Even under prudent operational control, a junior officer may quickly face a "use it or lose it" scenario during an Indian counteroffensive as the limited range of these systems requires them to be positioned close to the border, outside the hardened defenses of the rear garrisons.[96]

The final factor regards the potential impacts of LYNWs on the international intervention calculus. Both countries have adopted conventional military strategies that attempt to inflict (in India's case) or deflect (in Pakistan's case) as much conventional punishment as possible prior to international intervention.[97] India's Cold Start Doctrine, more recently labeled Proactive Strategy, seeks to rapidly conduct numerous limited military penetrations to secure Pakistani territory while remaining under the nuclear threshold.[98] Many South Asian scholars assert that this strategy was a major driver of Islamabad's push towards LYNWs, even though the strategy was never officially adopted by India.[99]

In response, Pakistan has since developed a strategy of New Concepts of Warfighting (NCWF) that seeks to "modernize, restructure and reposition its armed forces" to blunt Indian advances in conjunction with its LYNWs.[100] Former Pakistani Strategic Plans Division commander, retired Lt. Gen. Kahlid Kidwai claimed LYNWs were intended to "pour cold water on cold start."[101] What is most striking about both Indian and Pakistani war plans is the high emphasis on speed of execution. While on the surface this represents prudent military planning by both militaries to optimize force agility, these endeavors also critically limit decision space and de-escalation potential. The tempo of conflict that these strategies hope to achieve increases the potential for a rapid escalation sequence, while decreasing space for bilateral de-escalation measures to occur. Timely international intervention becomes more complicated under these expedited escalation timelines. There is also the potential that a military crisis under these conditions could unravel so quickly that an international intervention may not occur in time to prevent a nuclear first use.[102] Should this scenario play out, the prospects of convincing India to exercise restraint and withhold a strategic nuclear response against Pakistan become exceedingly slim. These issues, if left unchecked, may spell out the very nuclear disaster that many Western scholars adamantly fear, and with them, come a host of implications that will be explored further in the next section.

Implications for International Intervention

> *"While the prospects for direct coordination between the United States and other important third parties would be influenced by the nature of Washington's relations with these states, the United States should welcome this, and where possible, seek to cultivate such support and actively use it during crises. In its most coordinated form, the situation could amount to a 'collective actor' intervention where by a plurality of third parties coalesce and overcome their competitiveness to help achieve crisis de-escalation."*
>
> – Moeed Yusuf

The complex nature of the dynamics between India and Pakistan as nuclear-armed opponents poses unique risks on the world stage and foments distinctive challenges for the international community. International intervention is a calculated component by both India and Pakistan during these crises as a mechanism to draw in patron support.[103] This is exemplified by Mooed Yusuf who observed, "The predictability of U.S. crisis interventions also created a moral hazard problem and an incentive for Pakistan and India to manipulate the risk of war to attract Washington's attention and support."[104] This dichotomy demands a more multipolar approach with an emphasis on mediation to manage bilateral tensions and control incidents of potential escalation. Yusuf offers an insightful approach to this problem, which involves the use of third-party brokering techniques. All three military crises between India and Pakistan since declared nuclearization were dependent upon some form of third-party intervention to facilitate de-escalation.[105] The paragraphs that follow evaluate Yusuf's model,

explore the individual roles of the United States and China respectively, and conclude with a section exploring the prospects of a quadrilateral approach to future crises.

Yusuf relates brokered bargaining to a three-actor model that explains state behaviors during various crises.[106] The model is comprised of two parallel and intertwined interactions. The first involves the antagonists aiming actions and signals at one another in hopes of deterring an outcome or compelling them to respond in line with crisis objectives. The second involves luring the third party to act in certain ways while the intermediary attempts to find space to mediate to defuse the crisis.[107] These interactions ultimately lead to "an interplay of the perceptions, expectations, incentives, and strategies among the three parties that affects the overall behavior and stability, and in turn, the outcome of a crisis."[108] This results in a competition of sorts between the antagonists to obtain third-party support rather than a fear of a rebuke or third-party action against them.[109]

Yusuf's model did not specifically address Pakistan's pursuit of LYNWs and instead focused on de-escalation short of a descent into nuclear war. While this approach will certainly be the most prudent to prevent the use of such weapons short of all out mobilization, care must also be given to de-escalate quickly. Pakistan's development of a low-yield triad and its intent to leverage LYNWs as a means to lower the nuclear threshold also raises the potential for escalation to occur sooner in the conflict.[110] Traditional second-strike options require proactive deployment early in a crisis for survivability. Pakistan's development of nuclear-capable LYNWs for its existing fleet of *Agosta*-class submarines could stimulate the conditions for an early nuclear exchange.[111] Deployment of conventional and nuclear-tipped LYNW systems in and of itself, for example, could be enough to prompt India to escalate based on the fog-of-war scenario this situation would generate during an escalatory mobilization process. Public fear that such a scenario would invoke may also severely limit New Delhi's decision-making space and timing. The lack of an obvious solution to such problems, which the United States was also unable to solve during its LYNWs experience in Europe, increases the need for a shift and proactive intervention from the international community – most notably via the United States and China.

The United States has played a predominant role in the de-escalation process during previous crises in South Asia. It has been able to do this through a careful process of leveraging existing transactional partnerships with Pakistan while simultaneously appealing to India's desire to be perceived as a growing international power by urging New Delhi to exercise restraint.[112, 113] While this approach has worked well in the past, Washington's growing discord with Islamabad, namely over its alleged support to terrorism in Afghanistan, coupled with dwindling international aid, may reduce the clout of the United States during future intervention efforts.[114] Suspicions of impending strategic abandonment when the United States eventually reduces its commitments in Afghanistan, reminiscent of the scenario that played out following the Soviet occupation of Afghanistan, are probably also in the back of the Pakistani military leader's minds. Growing U.S. ties with India since 2005 and Pakistani fears of strategic encirclement via perceptions of a U.S. encouragement of an India-friendly Afghan government in

Kabul, have only further diminished the ability of the United States to influence Islamabad.[115] Inderjit Panjrath also alludes to the possibility that the bilateral relationship could even turn adversarial when he posited, "Pakistan's attitude towards the United States and its allies in Afghanistan may turn hostile – further exacerbating the already fragile situation and adding yet another dimension to the ongoing conflict in the region."[116] Collectively, these conditions are not promising and suggest the United States will have less influence over Pakistan during future crises.[117]

In stark contrast to the progressively declining relationship between the United States and Pakistan, China enjoys relatively close ties with Pakistan – a relationship that is growing stronger. Pakistan considers Beijing an "all-weather friend" and a reliable partner during a potential future conflict with India.[118] This sentiment is somewhat ironic as China is just as concerned as United States is about the potential for a nuclear war in South Asia, and would actively seek to avoid such an outcome to protect its rather substantial economic stakes in the subcontinent.[119] China has, and continues to make, significant investments in Pakistan to include assistance with its civilian nuclear power plants, various infrastructure improvement projects, the construction of the southern port of Gwadar, and most notably its $55 billion investment in the China-Pakistan Economic Corridor (CPEC) that will link Chinese imports/exports to the Arabian Sea.[120] It is also important to note that China was a key player in the progression of Pakistan's nuclear ambitions as it was a key supplier of its various delivery vehicles and assisted greatly in enhancing its indigenous missile production and fissile material production capabilities.[121] China also capitalized on the Soviet occupation of Afghanistan to expand its existing cooperation with Pakistan. However, with more lasting effect than its U.S. counterparts.[122] Of course, there is also the obvious common ground of seeking to curb India's expanding regional influence and economic growth, making Pakistan a perfect partner as a Chinese hedge against New Delhi. The aforementioned dynamics, coupled with already deep historical ties, will make China a more feasible third-party broker with Pakistan during future crises.

The evolving geopolitical landscape and the progressive realignment of traditional patron relationships in the region may mandate a different strategy and suggests a quadrilateral approach may be a more appropriate response to future South Asian crises. China's strong influence with Pakistan, and its desire to prevent a potential escalation that risks nuclear war, makes Beijing a viable broker for Islamabad. Conversely, growing relations between the United States and India may be leveraged effectively to represent a viable third-party broker for India. In this light, a four-party de-escalation process could prove to be a feasible method of international intervention in the future.

Splitting up the responsibilities of crisis monitoring, *in extremis* bilateral intelligence-sharing channels could potentially be preestablished between the United States and China to address the rapid de-escalation requirements that will be inherent to the introduction of LYNWs. While not an ideal situation as there are trust barriers between Beijing and Washington, sharing of sanitized information in a timely manner is certainly better than the alternative of idly watching a rapid and

uncontrolled escalation unfold. Preemptive formation of intervention delegation parties by the United States and China with rough outlines of prepared material to aid in the mediation process may be effective. This could be a more comprehensive version of the "notional playbook" the United States utilized during the Mumbai crisis, which had been developed during the previous two India-Pakistan crises since declared nuclearization.[123]

Opportunities

Despite a negative trajectory towards the revival of LYNWs within the nuclear domain, there are avenues the international community could explore to address South Asian issues.[124] The opportunities should come from the international community writ large, not the United States specifically, due to the fact that U.S. credibility with Pakistan has waned as Washington has placed its burgeoning relationship with New Delhi on full display.[125] Perceptions of preferential treatment by the United States towards India render the United States a biased broker in the Pakistani view. As such, other players on the international stage should be encouraged to take more proactive roles in the process to diffuse tensions in South Asia. These include obvious players such as China, who shares a stronger patron relationship with Pakistan, but also other regional actors such as Sri Lanka, Bangladesh, and Nepal who also have much to lose in the event of a nuclear war. Russia is another possibility as Moscow shares historic defense ties with India and a growing relationship with Pakistan. Under these premises, two opportunities are presented for consideration: steering Pakistan towards a safer employment of LYNWs through international collaboration on training, education, and lessons learned, and establishing a viable international mediation forum for India and Pakistan to address enduring bilateral issues such as the Kashmir issue, water sharing agreements, and cross-border violence.

The window to dissuade Pakistan away from the prospect of LYNWs has already closed. A U.S. or international rebuke now would be deemed hypocritical and dismissed by the Pakistanis given how the United States recently reconsidered LYNWs. However, symposiums and other discussions with Islamabad using declassified material about the intricacies of the LYNW experience in Europe may help Islamabad shape its decisions regarding LYNW architecture in a constructive and informed manner. This is already occurring to some extent through the multi-track talks, but these efforts should be expanded.[126] This may address some of the previously stated issues of Pakistan walking away with the wrong end-states and lessons learned about LYNWs in Europe based upon their limited consumption of Western scholarship. These discussions should occur in a coalition-based setting and include not just the nuclear-armed nations, but countries in Europe that housed elements of the NATO nuclear contingent as these countries offer unique perspectives – particularly regarding the downsides of such systems.[127]

The United States and the larger international community have been reticent to officially acknowledge standing territorial issues between India and Pakistan as anything more than bilateral in nature. Ironically, this is the most consistent U.S. policy position in South Asia. However, it is exceedingly clear that bilateral

mediation efforts have failed and the numerous deep-seated issues between the two countries will require international mediation for any meaningful progress to occur. If South Asia represents the most likely environment for a nuclear war, then it stands to reason that the most effective way to prevent such an outcome is to address the core friction points that would incite a nuclear confrontation. Establishing an international forum for Pakistan and India to address their concerns accomplishes two things. It provides international legitimacy to these issues and it provides a venue to vent during periods of heightened tensions. This could potentially provide a valuable de-escalation offramp during a crisis as it would give both sides the ability to pause and bring issues to the international courts instead of depending on international intervention to bring them back from the precipice. Previous crises since declared nuclearization (Kargil in 1999, the 2001-2002 Op Parakram Crisis, and Mumbai in 2008) demonstrated that established routes of bilateral de-escalation through hotlines are only effective to a point, and that both sides have habitually abandoned military and political dialogue when the stakes are at their highest.

Conclusion

The enormous challenges in South Asia represent wicked problems on the international stage with no easy or clear solution in sight. These challenges are complicated by waning American influence with Pakistan and the increasingly complex regional dynamics that will demand multinational mediation approaches that include other powers such as China and perhaps Russia. The introduction of LYNWs to an already extremely tense environment will undoubtedly create great consternation among the various global powers and regional actors. However, the nuclear restraint that binds together the nuclear-armed powers of the world has continued to hold despite crises, accidents, and miscalculations.[128] The great South Asian nuclear rivalry between Pakistan and India has produced several close calls but both states have navigated these crises without resorting to nuclear war, albeit with some outside mediation assistance.[129] Despite numerous provocations, India has exercised strategic restraint and Pakistan, whether purposefully or by accident, has avoided pushing the envelope too far. These factors would lead nuclear optimists to conclude that both countries have developed enough sense of one another to sufficiently weather the storm of escalation, much like the United States and the Soviets during the Cold War. However, there are staunch differences between the Cold War nuclear environment and the South Asian one. The United States and the Soviet Union had not engaged in three major conflicts against one another. They were not geographically contiguous states, and the military asymmetry between the United States and the Soviets during that period was not as pronounced as that between Pakistan and India today.

The prospects of a limited nuclear war are just as grim today as they were when LYNWs were first introduced. However, these weapons successfully deterred Soviet aggression in Europe and the nuclear taboo endured. While unhelpful for regional stability, it is reasonable that Pakistan has reached similar conclusions. In the absence of quantitative or qualitative conventional parity, which in all likelihood will never come irrespective of Islamabad's monetary commitments,

military acquisitions, or efforts to modernize, it is not surprising that Pakistan turned to its nuclear arsenal to safeguard its sovereignty. While there is certainly cause for concern regarding the prospect of nuclear war in South Asia, particularly with the introduction of LYNWs, the situation is not without hope. Bringing South Asia into nuclear norms, creating constructive opportunities to address major friction points, and a supportive international community will go a long way towards defusing future tensions.

Chapter 2 Notes

1. Gurmeet Kanwal, Sharpening the Arsenal: India's Evolving Nuclear Deterrence Policy (Uttar Pradesh, India: Replika Press Pvt Ltd and HarperCollins Publishers, 2017), pps. 86-89.

2. Mark Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers* (New York, N.Y.: International Institute for Strategic Studies, Routledge Taylor, and Francis Group, 2014). Pps. 16-17.

3. Ibid., pps. 159-164.

4. V. Sahay, *Tactical Nuclear Weapons Deterrence Stability Between India and Pakistan* (New Delhi, India: Gaurav Book Centre, 2018), p. 30; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, pps. 31-33.

5. Inderjit Panjrath, *Pakistan's Tactical Nuclear Weapons* (New Delhi, India; Vij Books India Pvt Ltd., United Service Institution of India, 2018), p. 19; Vipin Narang, *Nuclear Strategy in the Modern Era, Regional Powers and International Conflict* (Princeton, N.J.: Princeton University Press, 2014), p. 81; Bhumitra Chakma, *Pakistan's Nuclear Weapons* (New York, N.Y.: Routledge Taylor and Francis Group, 2009). P. 52.

6. Tom Nichols, Douglas Stuart, and Jeffrey McCausland, *Tactical Nuclear Weapons and NATO* (Carlisle, Pa.: Army War College, Strategic Studies Institute, April 2012) pps. Viii-ix.

7. David O. Smith, "The US Experience with Tactical Nuclear Weapons: Lessons for South Asia," Paper written with the Stimson Center, p. 8.

8. Ibid., p 7.

9. Eric Schlosser, *Command and Control* (New York, N.Y.: Penguin Books, 2013), pps. 245-249.

10. Smith, "The US Experience with Tactical Nuclear Weapons," pps. 14 and 23.

11. Ibid., pps. 14 and 23.

12. Ibid., p. 18.

13. Nichols, et al., *Tactical Nuclear Weapons and NATO*, p. 7.

14. Panjrath, *Pakistan's Tactical Nuclear Weapons*, pps. 5 and 18.

15. Sadia Tasleem and Tony Dalton, "Nuclear Emulation: Pakistan's Nuclear Trajectory," *The Washington Quarterly*, Winter 2019, p. 143.

16. Sannia Abdullah, "Nuclear Ethics? Why Pakistan Has Not Used Nuclear Weapons…Yet," *The Washington Quarterly*, Winter 2019, p. 165.

17. Tasleem and Dalton, "Nuclear Emulation," p. 144.

18. Smith, "The US Experience with Tactical Nuclear Weapons," pps. 22-23.

19. Chakma, *Pakistan's Nuclear Weapons*, p. 40.

20. Kanwal, *Sharpening the Arsenal*, p. 16.

21. Chakma, *Pakistan's Nuclear Weapons,* p. 47.

22. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 51; Chakma, *Pakistan's Nuclear Weapons,* p. 79.

23. Chakma, *Pakistan's Nuclear Weapons,* p. 46.

24. Ibid., p. 51.

25. Panjrath, *Pakistan's Tactical Nuclear Weapons,* p. 34; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 92; Tasleem and Dalton, "Nuclear Emulation," p. 138.

26. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, pps. 22-24 and 71-73; V.N. Veda, *Pakistan's Nuclear Weapons* (New Delhi, India: Centre for Air Power Studies, KW Publishers Pvt Ltd, 2012), p. 25.

27. Kanwal, *Sharpening the Arsenal,* p. 50.

28. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 85.

29. Chakma, *Pakistan's Nuclear Weapons,* p. 56.

30. Narang, *Nuclear Strategy in the Modern Era,* p. 55.

31. Ibid., p. 56.

32. Chakma, *Pakistan's Nuclear Weapons,* p. 60.

33. Narang, *Nuclear Strategy in the Modern Era,* pps. 86-87; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers,* p. 26; Panjrath, *Pakistan's Tactical Nuclear Weapons,* pps. 44-45.

34. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 90.

35. Hans M. Kristensen, Robert S. Norris, and Julia Diamond, "Pakistani Nuclear Forces, 2018," *Bulletin of the Atomic Scientists*, 2018, p. 349, accessed Sept. 8, 2018, at https://doi.org/10.1080/00963402.2018.1507796.

36. Ashley J. Tellis, *India's Emerging Nuclear Posture: Between Recessed Deterrent and Ready Arsenal* (Santa Monica, Calif.: RAND Corporation, 2001), p. 251.

37. Ibid., p. 251.

38. Ibid., pps. 252-253.

39. Ibid., p. 253.

40. Ibid., p. 254.

41. Narang, *Nuclear Strategy in the Modern Era*, p. 100.

42 Ibid., p. 100.

43. Tellis, *India's Emerging Nuclear Posture*, p. 302.

44. Ibid., pps. 374-378.

45. Chakma, *Pakistan's Nuclear Weapons,* p. 49.

46. Tellis, *India's Emerging Nuclear Posture*, pps. 312-313.

47. Ibid., p. 321.

48. Ibid., pps. 342-344.

49. Ibid., p. 342.

50. Ibid., p. 347.

51. Narang, *Nuclear Strategy in the Modern Era,* pps. 95-95.

52. Ibid.

53. Hans M. Kristensen and Robert S. Norris, "Indian Nuclear Forces, 2017," *Bulletin of the Atomic Scientists*, 2017, p. 206, accessed Sept. 8, 2018, at https://doi.org/10.1080/00963402.2018.1507796.

54. Moeed Yusuf, *Brokering Peace in Nuclear Environments* (Redwood City, Calif.: Stanford University Press, 2018), p. 158.

55. Yusuf, *Brokering Peace in Nuclear Environments,* p. 171; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers,* p. 65.

56. Jeffrey Larsen and Kerry Kartchner, *On Limited Nuclear War in the 21st Centur*y (Redwood City, Calif.: Stanford University Press, 2014), p. 107; Tasleem and Dalton, "Nuclear Emulation," pps. 140-141; Meenakshi Sood, "Pakistan's Response to Cold Start Doctrine," Centre for Land Warfare Studies, Issue 94, March 2017, pps. 1-3.

57. Panjrath, *Pakistan's Tactical Nuclear Weapons,* p. 44.

58. Smith, "The US Experience with Tactical Nuclear Weapons," p. 4.

59. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, pps. 119 and 124-125; Narang, *Nuclear Strategy in the Modern Era*, pps. 86-87.

60. Narang, *Nuclear Strategy in the Modern Era,* pps. 86-87.

61. Sagan and Kenneth Waltz, *The Spread of Nuclear Weapons: An Enduring Debate* (New York, N.Y.: W.W. Norton & Company, 2013), p. 2

62. Panjrath, *Pakistan's Tactical Nuclear Weapons,* p. 5.

63. Todd S. Sechser and Matthew Fuhrmann, *Nuclear Weapons and Coercive Diplomacy* (New York, N.Y.; Cambridge University Press, 2017), p. 121.

64 Larsen and Kartchner, *On Limited Nuclear War in the 21st Centur*y, p. 108; Sechser and Fuhrmann, *Nuclear Weapons and Coercive Diplomacy*, p. 149.

65. Kanwal, *Sharpening the Arsenal,* pps. 17-25.

66. Panjrath, *Pakistan's Tactical Nuclear Weapons,* p. 37; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 86; Kanwal, *Sharpening the Arsenal*, p. 31.

67. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 77.

68. Sahay, *Tactical Nuclear Weapons Deterrence Stability Between India and Pakistan*, pps. 12-23; Kanwal, *Sharpening the Arsenal,* pps. 123-132.

69. Narang, *Nuclear Strategy in the Modern Era*, pps. 103-104.

70. Kanwal, *Sharpening the Arsenal,* pps. 10 and 32.

71. Panjrath, *Pakistan's Tactical Nuclear Weapons,* pps. 47-48.

72. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 34; Panjrath, *Pakistan's Tactical Nuclear Weapons*, pps. 47-48.

73. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 34; Panjrath, *Pakistan's Tactical Nuclear Weapons,* p. 46.

74. Panjrath, *Pakistan's Tactical Nuclear Weapons,* p. 49.

75. Ibid., p. 61.

76. Kanwal, *Sharpening the Arsenal,* p. 13; Sechser and Fuhrmann, *Nuclear Weapons and Coercive Diplomacy*, pps. 36 and 150.

77. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 49.

78. Panjrath, *Pakistan's Tactical Nuclear Weapons,* p. 61.

79. Kanwal, *Sharpening the Arsenal,* p. 32.

80. Panjrath, *Pakistan's Tactical Nuclear Weapons,* pps. 46-49; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 34.

81. Panjrath, *Pakistan's Tactical Nuclear Weapons*, pps. 46-49; Narang, *Nuclear Strategy in the Modern Era*, pps. 86-87; Chakma, *Pakistan's Nuclear Weapons,* p. 78.

82. Panjrath, *Pakistan's Tactical Nuclear Weapons,* p. 61.

83. Kanwal, *Sharpening the Arsenal,* pps. 7 and 50; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 75.

84. Kanwal, *Sharpening the Arsenal,* pps. 13, 17, and 25.

85. Narang, *Nuclear Strategy in the Modern Era*, p. 111.

86. Smith, "The US Experience with Tactical Nuclear Weapons," p. 10.

87. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, pps. 26 and 84-85.

88. Kanwal, *Sharpening the Arsenal,* p. 17.

89. Abdullah, "Nuclear Ethics?," p. 159.

90. Tasleem and Dalton, "Nuclear Emulation," p. 150.

91. Narang, *Nuclear Strategy in the Modern Era*, p. 85.

92. Smith, "The US Experience with Tactical Nuclear Weapons," p. 40.

93. Ibid., p. 44.

94. Veda, *Pakistan's Nuclear Weapons*, p. 49, 60, and 70; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, pps. 126 and 132.

95. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 89.

96. Chakma, *Pakistan's Nuclear Weapons,* p. 79; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, pps. 85 and 89.

97. Sood, "Pakistan's Response to Cold Start Doctrine," p. 2.

98. Larsen and Kartchner, *On Limited Nuclear War in the 21st Centu*ry, p. 107; Tasleem and Dalton, "Nuclear Emulation," pps. 140-141; Sood, "Pakistan's Response to Cold Start Doctrine," pps. 1-3.

99. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 80.

100. Panjrath, *Pakistan's Tactical Nuclear Weapons,* pps. 5 and 18.

101. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 81; Panjrath, *Pakistan's Tactical Nuclear Weapons*, p. 21.

102. Yusuf, *Brokering Peace in Nuclear Environments,* pps. 178-179.

103. Yusuf, *Brokering Peace in Nuclear Environments,* p. 23.

104. Ibid., p. 158.

105. Ibid., p. 158.

106. Ibid., p. 28.

107. Ibid., pps. 40-41.

108. Ibid., p. 40.

109. Ibid., p. 42.

110. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 26; Sood, "Pakistan's Response to Cold Start Doctrine," p. 6.

111. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 26; Narang, *Nuclear Strategy in the Modern Era*, pps. 108-109.

112. Panjrath, *Pakistan's Tactical Nuclear Weapons,* p. 71.

113. Kanwal, *Sharpening the Arsenal*, p. 32.

114. Veda, *Pakistan's Nuclear Weapons*, p. 50.

115. Panjrath, *Pakistan's Tactical Nuclear Weapons,* p. 72.

116. Ibid., p. 72.

117. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 66.

118. Veda, *Pakistan's Nuclear Weapons*, p. 2.

119. Panjrath, *Pakistan's Tactical Nuclear Weapons*, ps. 71.

120. Ibid., pps. 71-74.

121. Veda, *Pakistan's Nuclear Weapons*, pps. 2 and 35; Chakma, *Pakistan's Nuclear Weapons*, p. 28.

122. Chakma, *Pakistan's Nuclear Weapons*, p. 28.

123. Yusuf, *Brokering Peace in Nuclear Environments*, p. 140.

124. Amy F. Woolf, "Nonstrategic Nuclear Weapons," Congressional Research Service Report, January 2017. Pps. 1-2.

125. Panjrath, *Pakistan's Tactical Nuclear Weapons*, p. 72.

126. Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, p. 66.

127. Smith, "The US Experience with Tactical Nuclear Weapons," pps. 9-10.

128. Abdullah. "Nuclear Ethics?," p. 158.

129. Yusuf, *Brokering Peace in Nuclear Environments*, p. 24.

CHAPTER 3

Entanglement Risks and Nuclear Deterrence Theory

Colonel Anthony T. Shafer, Jr. U.S. Air Force

During the Cuban Missile Crisis in 1962, the United States was concerned that Soviet submarines could jeopardize or attack U.S. blockade forces. The U.S. Navy was ordered to track Soviet submarines in the area and force them to surface. While executing the blockade, the U.S. Navy used a standard procedure of depth charges to signal Soviet submarines needed to surface. However, this signal was confusing to the submarine crews. Due to intermittent communication with their headquarters in Moscow and unsure of the nature of the depth charges being employed against them, tensions rose. What the U.S. Navy did not understand was that some Soviet submarines were armed with 15 kiloton nuclear-tipped torpedoes and the crews were delegated employment authority under specified circumstances. In this instance, the United States targeted what it believed to be a conventionally-armed submarine when it was actually nuclear armed.[1] The elevated tensions of the Cuban Missile Crisis made the attempted surfacing of these submarines by depth charges risky and escalatory. The incident could have led to a single submarine captain firing a nuclear torpedo, likely destroying both American and Soviet naval forces in the area, and as likely, leading to nuclear war. The submarine armed with both nuclear and conventional weapons is an example of a dual-use system and the events described above exemplifies entanglement.

Many scholars have commented on the growing risk of nuclear conflict due to entanglement of strategic systems and conventional systems. While this is not a new concern, many believe the risks have increased recently due to many reasons including technological advances, war fighting in the new domains of space and cyberspace, and nuclear policies and doctrine. Further, proliferation forces U.S. policymakers today to consider nuclear escalation risks across a spectrum of nuclear-armed states from small to superpower-sized arsenals. This paper argues deterrence theory suggests that because technological advancements have made nuclear arsenals more vulnerable to counterforce attack and entanglement more likely, in some cases, a state's nuclear posture, its arsenal size and composition

could make purposeful entanglement a credible deterrent against conventional attacks.

This paper begins by outlining the research question, hypothesis and research methodology used. The paper then begins a literature review defining entanglement and entanglement risks. It also reviews the current literature regarding increased entanglement risks due to technological advances, before considering deterrence theory literature to further understand entanglement. The paper then considers interactions of nuclear deterrence postures with entanglement as well as how the stability instability paradox relates to entanglement. After the literature review, the paper argues the hypothesis is supported as technological advances, specific nuclear postures and nuclear arsenal sizes make intentional entanglement a credible option for some nations to deter conventional attack. Finally, the paper provides recommendations to U.S. policymakers and planners based on the paper's understanding that intentional entanglement to deter conventional attack is possible and, in some instances, likely.

Research Question, Hypothesis and Methodology

This paper argues that deterrence theory suggests that because technological advancements have made nuclear arsenals more vulnerable to counterforce attack, state nuclear postures and size makes purposeful entanglement a credible deterrent against conventional attack. The thesis centers around the research question of how deterrence theory interacts with and informs modern entanglement risks. The paper draws on theory posed by classic deterrent theorists as well as contemporaries. The paper also leverages work by James Acton, Caitlan Talmadge, and Barry Posen to understand the effects of technology on entanglement.

The paper provides an understanding of entanglement risks based on the study of deterrence theory and how deterrence theory can inform policymakers and planners regarding entanglement. The paper seeks to confirm the hypothesis that entanglement could be beneficial to states with small nuclear arsenals and with limited conventional capabilities who practice specific deterrent postures. If confirmed, American planners would be wise to understand in what instances nations might seek to deter conventional aggression by entangling their nuclear and conventional systems.

This paper uses qualitative analysis of existing theory and information regarding entanglement. The paper also reviews the existing body of deterrence theory and applies it to the idea of entanglement. Deterrence theory is used to draw a more complete understanding of what causes entanglement, what variables change the entanglement risks and which variables change credibility of the entanglement risks. The qualitative analysis provides a basis to conclude what situations intentional entanglement could be beneficial to national goals.

It is important to scope the nature of escalation and what inadvertent escalation is from the outset. Escalation to nuclear conflict during a conventional war could imply increasing the readiness posture of strategic forces, by placing them on alert, transferring weapons from storage to more operational settings or removing safeguards. At the farther end, nuclear escalation could include a

recallable demonstration, like alerting or even launching fighter-bombers with nuclear weapons, threatening their use up to both limited and total war.[2] Inadvertent escalation due to entanglement is the idea that two nuclear nations at conflict could inadvertently escalate the conflict to nuclear war, even if both sides preferred to keep the conflict conventional.

Technology and Cyber Increasing Entanglement Escalation Risks

The rate of technical change including the emerging importance of both the cyber and space domains makes entanglement and the risks of escalation during conventional conflict between nuclear powers more likely. At the center of these new and growing risks of entanglement, is the idea that new technologies offer counterforce options making nuclear forces vulnerable to attack as well as new domains and technologies that are less widely understood by policymakers and operators.[3]

A primary concern that increases entanglement risks are improvements to nuclear and conventional weapon systems that offer a realistic chance of a devastating first use counterforce attack. Such an attack could remove an adversary's ability to respond to a nuclear attack with its nuclear deterrent. Keir A. Lieber and Darryl G. Press articulated these technical improvements along several lines. First, they discuss improvements to surveillance. Missiles are most vulnerable prior to launch, making an ability to find and fix them key to a counterforce strike. Surveillance improvement due to technical advances could mitigate advantages found in missiles that use concealment and mobility to avoid being targeted prior to launch by adversaries. New surveillance systems could track mobile intercontinental ballistic missile (ICBM) and submarine-launched ballistic missile (SLBM) systems found in the Chinese arsenal. Further, improvements to sea surveillance may soon render even the most advanced and quiet submarines unable to hide.[4] Once exposed, submarines would be nearly defenseless.

Lieber and Press also discuss improvements in weapons accuracy, targeting and fusing. Improved accuracy of SLBMs show that perhaps these weapons heretofore used as punishment weapons against population centers, could now be used against fielded nuclear forces in a counterforce role. Further, improvements to fusing allows exquisitely fine-tuned timing to hold hardened targets such as ICBMs buried within silos, to be effectively destroyed.[5]

As a result of these technological advances, important elements of a state's deterrent are held at greater risk and could be eliminated early in any conflict. From an entanglement standpoint, vulnerability of nuclear forces due to surveillance, accuracy and targeting, changes the way an adversary could perceive accidental encroachments on nuclear systems. If adversaries believe their nuclear deterrence is vulnerable due to these technical improvements, they would be more concerned in the event an entanglement scenario were to threaten any aspect of the deterrent. In a classic security dilemma, technological developments providing counterforce possibilities are destabilizing until the threatened state can field countermeasures.

However, until such time, adversarial technical improvements intensify risks during limited conventional conflict. Further, if a state believes an adversary possesses a counterforce capability against its nuclear deterrent, that state would be more likely to interpret any incursion due to entanglement as purposeful rather than accidental. Compounding the misinterpretation issue, states facing a perceived counterforce capable adversary is more likely to execute a preemptive first strike fearing waiting could remove their ability to do so.[6]

A second concern is that these new technologies effect states differently depending on the resources available. A state with little resources to develop countermeasures to new technologies or that has a small nuclear arsenal that is not hardened and dispersed like the U.S. triad would be less likely to absorb an attack using these new technologies while maintaining its assured retaliation ability.[7]

From an entanglement standpoint, these technological improvements add credibility to a state's claim that an attack on its dual-use entangled systems is escalatory and will become even more credible in the future as counterforce technologies improve. Further technological advances will provide more credibility for states whose nuclear deterrent is more vulnerable to an attack because of the size and make up of their nuclear arsenal.

Increased Dependency in Space and Cyber Space

The increased use and dependency of space and cyber domains for nuclear systems has also increased the likelihood of entanglement escalation. For years, concerns over the nuclear enterprise's security vis-a-vis cyberthreats has loomed. In 2013, the Department of Defense Science Board found that many military weapons systems were vulnerable and unprepared for cyberattacks.[8] Further, a recent report by the Cyber Nuclear Weapons Group, repeated this warning saying, "A successful cyberattack on nuclear weapons or related systems – including nuclear planning systems, early warning systems, communication systems, and delivery systems, in addition to the nuclear weapons themselves (collectively, nuclear weapons systems) could have catastrophic consequences."[9]

There are several unique considerations of cyberwarfare and entanglement. First, the low cost of entrance means many nonstate organizations are and will continue to participate in cyberwarfare. Secondly, cyberattacks are sometimes difficult to attribute to an attacker. Further, first-world infrastructure, military systems, and economic activities continue to be increasingly reliant on cyber systems, thus increasing the impacts of cyberattacks.[10] States prosecuting cyberattacks on other nuclear states could inadvertently affect strategic systems via the cyberattack, leading to entanglement escalation. Finally, both cyber and space are immensely technical and complex by their nature. It is unlikely senior military or government officials will fully understand or anticipate second- and third-order effects of conflict in these domains and their effects on entanglement and escalation.

Cyber entanglement concerns take two forms. First, as discussed above, is a classic entanglement situation through either targeting of a dual-use system for conventional gain or via collateral damage. A second entanglement risk possibility

is a cyberattack launched on entangled systems that could be misunderstood as a prelude to a strategic attack by an adversary, but was actually committed by a nonstate actor or technical failure. While extremely unlikely, a risk of nonstate interference adds to fog and friction of war and must be considered during conflict between two states. While most experts agree nonstate, actors do not currently possess the sophistication needed to generate an attack on a nuclear state's nuclear command, control, and communications (NC3) this type of spoofing third-party attack remains a possibility.[11]

Both cyber and space have increased entanglement risks due to complexities and ambiguities as well as the speed and vulnerability of operations within them. For example, non-kinetic and reversible attacks are especially likely in both cyber and space domains.[12, 13] Denial type attacks could impair systems temporarily. Denial of service cyberattack of computer and other communications systems is one example. For space, a reversible denial attack could be accomplished with jamming or intercepting communications between space systems or between space and ground sites, as well as dazzling space-based imagers. A third consideration especially relevant to space attack is collateral damage. If for example, an anti-satellite (ASAT) weapon is employed against a space asset, depending on the orbit, and other specifics, there is potential for significant collateral damage to other space assets in the same orbit.[14] The sum effect of these cyber trends means entangled strategic systems are now more vulnerable to attack while recovery and attribution from such an attack is more difficult. For policymakers, these new domains add credibility to a state arguing that attack on dual-use cyber or space systems would be escalatory.

Deterrence Theory and Entanglement

In applying deterrence theory to entanglement, one must first consider if the entanglement risks are understood by adversaries. If risks are understood, two concepts should be considered by belligerents – tripwires and credibility.

The best-known examples of tripwires are a tripwire force. During the Cold War, American personnel were posted in Europe in large part to ensure any conflict in Europe would place American personnel at risk. By having personnel directly at risk if war started, the United States gained credibility that it would respond to aggression from the Soviet Union in Europe. In this way, the tripwire force assured allies that the United States was committed to Europe and NATO.[15]

The second type of entanglement problem involves entanglement risks adversaries don't understand or anticipate. With respect to entanglement, there are many examples of tripwires in today's modern nuclear arsenals. A present-day example of a known entanglement risk as a tripwire is the Space-Based Infrared System (SBIRS), the U.S. early warning satellite system. James Acton provides an excellent example using U.S. SBIRS. Because SBIRS is able to track both nuclear and conventional ICBMs, it is a dual-use system and thus entangled. Consider that China has both conventional and nuclear-armed missiles. In a conventional war with the United States, both would want to disable SBIRS to increase the likelihood that a conventional missile attack against the United States would be successful.

However, such an attack would be escalatory, because it also degrades the U.S. ability to defend against a nuclear attack. In this case, the SBIRS system could be considered a tripwire. While this specific system was not mentioned directly, the 2018 *Nuclear Posture Review* (NPR) does state that the United States will consider strategic retaliation even for nonstrategic attacks on NC3 systems, such as SBIRS.[16]

In this case, because of entanglement, adversaries must consider if the mission risk of not attacking SBIRS prior to a conventional ICBM attack on the United States, outweighs the potential escalation risk to nuclear war that striking the SBIRS system might have. When the attacking state believes the escalation risk is too great, entanglement has provided a deterrent from attack. Compounding this effect is the belief many experts have that entanglement risks have increased in recent years based on technology and doctrine changes.[17] If this is correct, nuclear-armed states must now consider an entanglement risk calculation across a multitude of systems correctly before initiating a conventional conflict.

Tripwires in this context is slightly different than in traditional nuclear deterrence theory. For Thomas Schelling and other early deterrence theorists, tripwires were purposefully placed to force an attacker to consider the likelihood that an attack would be escalatory. "We have developed the idea of making a threat credible by getting ourselves committed to its fulfillment, through the stretching of a 'tripwire' across the enemy's path of advance"[18] In entanglement, these tripwires might be purposeful, but are as likely not. Purposeful or not, tripwires due to dual-use systems and entanglement lead to escalation. Considering the discussion above regarding space, SBIRS is entangled because Chinese rockets are dual-use capable and SBIRS tracks those rockets regardless of the warhead arming it. Purposeful or not, tripwires due to dual-use systems and entanglement lead to escalation making their result similar in both entanglement and deterrence theory contexts.

Belligerents understanding an entanglement risk of a given system does not necessarily make the associated system a tripwire. Credibility must also be considered. Credibility in this case means how reasonable one is to conclude that attacking a known dual-use system would cause the conflict to escalate. Credibility is affected by several factors. First, how critical is the system to the state's nuclear deterrent? For example, Acton argues that U.S. NC3 has become less redundant relying on increasingly fewer systems and subsystems.[19] In this example, the lack, of redundancy within NC3 improves the credibility that targeting the known entanglement risk would likely escalate the conflict because the loss of the specific scarce system would remove capability within the nuclear deterrent. On the other hand, when considering vastly redundant systems, a state could possibly absorb degradation of a strategic system without critically diminishing the effectiveness of its nuclear deterrent.

The vulnerability of the system and the type of attacks used also affect credibility. Systems highly vulnerable to direct kinetic attack would likely be less credibly escalatory versus hardened and dispersed systems. Similarly, systems attacked via non-kinetic or reversible means would likely be less credible than kinetic attacks that destroy systems. However, credibility calculations regarding entanglement are highly subjective, complex, and specific to individual systems.

Further, attacked states and attacking states are likely to reach differing conclusions than attacked states regarding the same entangled dual-use system.

Additionally, credibility would be affected by the size of a state's nuclear arsenal and its survivability. If a known entangled system was targeted during a conventional attack, states with large, complex dyads or triads would be more likely to be able to withstand the strike and maintain their assured second-strike capability. Therefore, the escalation risk is less credible for these states and entanglement less likely to deter conventional aggression. For states with smaller or more vulnerable nuclear forces, any attack of a dual-use system would be more critical, particularly if the state believed its ability to retaliate is being degraded.

Finally, states can increase credibility that targeting dual-use systems would be escalatory through strategic messaging. The United States and Russia have done this in the past by make the treaties that established the importance of space-based early warning to stability.[20] Further, the 2018 *Nuclear Posture Review* has explicitly said targeting of NC3 systems could trigger a strategic response.[21]

The second type of entanglement problem involves entanglement risks that adversaries don't understand or anticipate. In unknown entanglement, adversaries will not understand the pressures they are putting on each other's nuclear deterrent during conventional confrontations. Brinksmanship best describes the scenario where two nuclear powers are engaged in conventional conflict and do not understand the entanglement risks the operations within the conflict are incurring. In the context of entanglement, brinkmanship entails the idea that two nuclear countries may not be able to maintain a limited conventional war because a dual-use system could inadvertently be targeted leading to escalation. Unintended entanglement escalation involves an element of unknown consequences and loss of an ability to control escalation by state leaders. Schelling described brinksmanship as two climbers tied together with a rope. If either falls, they will both fall. While neither could credibly threaten the other, there is much left to chance, like loose gravel, dizziness, or something else that in that situation could lead to both people falling. Put another way, brinksmanship allows some amount of risk to be left to chance.[22] Again, there are several factors to consider for unknown entanglement risks. Based on the discussion at the beginning of the paper, reliance on space and cyber technologies make this type of entanglement more likely because of the complexity of operations in these domains. Further, the number and degree of diversification of a state's nuclear weapons, as well as its posture are also factors. A state considering an attack on another nuclear-armed state must consider both known and unknown entanglement threats to fully understand the risk the conventional action poses.

Like the example of a U.S.-China conflict discussed above, China could see its entangled conventional and nuclear command, control, and communications attacked. After such an attack, China might surmise its nuclear deterrent will not be available if they continued to wait and would therefore consider escalating the conflict, initiating the first use of nuclear weapons.[23] The relationship between entanglement and brinkmanship is further amplified because of advances in space, cyber and conventional technologies. NC3 as well as other nuclear operations largely leverage the space and cyber domains. Cyber, in particular, is difficult for

noncyber experts to fully understand. As mentioned above, cyber also potentially presents ambiguity in three ways. First, in general, cyberattacks are harder to attribute to an actor. Secondly, cyber being more accessible than other weapons to nonstate actors, it is plausible a nonstate actor either unknowingly or with the goal of escalating the tensions between the states in conflict deployed a cyberattack.[24] Finally, a cyberattack targeting one system could spill to another system causing collateral damage.[25]

Lastly, because the entanglement risk is unknown to adversaries, once targeted, an attacked state might wish to accentuate unknown threats by reacting to and making known the entanglement encroachment by the aggressor. Reaction could be alerting nuclear forces or alert levels, while messaging to the aggressor that a threshold had been crossed.[26] Further, once tensions rise or conflict actually begins, the fog of war increases because of limiting intelligence collection and processing that can take place during conflict. Each side will attempt to limit and degrade intelligence, surveillance, and reconnaissance (ISR). Additionally, as operations become more secretive, increased suspicions are more likely to lead to the belligerents suspecting the other of a massive first-strike attack.[27] The combination of an escalation misstep that has led to conflict escalation already along with degraded ISR capabilities as normal course, would reinforce the idea of brinkmanship.

Relationship between Nuclear Posture and Entanglement

It is useful to consider entanglement in relation to a state's nuclear posture. Vipin Narang, discusses nuclear posture extensively in his book *Nuclear Strategy in the Modern Era*. He offers that superpowers have the ability to pursue both first use and assured retaliation policies and that historical doctrine of the United States and the Soviet Union or Russia such as mutually assured destruction (MAD), flexible response and others, were variations of preference to first use from second strike and vice versa.[28] Further, Barry Posen asserts that problems of entanglement "loom especially large for small- and medium-sized nuclear powers since they have the most difficult time building forces that can survive."[29] The corollary would also be true. Superpowers are somewhat insulated from entanglement pressures because of their ability to survive a first strike with an assured response capability intact. Finally, as discussed above, Lieber and Press point out how technological advances in counterforce capabilities effect nuclear powers differently. States with sufficient resources and technical abilities can maintain a reliable and credible second-strike deterrent despite technological advances, by developing and employing countermeasures. This is not the same for many countries with less developed capabilities, giving superpowers more asymmetric advantages regarding nuclear capabilities.[30] Finally, improvements to counterforce technologies will likely push policymakers away from further reductions of nuclear forces.[31] Technological improvements to nonnuclear counterforce capabilities hold both the American- and Russian-fielded nuclear forces more at risk than they were even a few years ago. As technologies mature, they will be even more at risk in the future, making further reductions in nuclear arsenals riskier.[32]

Narang describes three postures regional nuclear powers pursue. These postures describe nuclear deterrence and are worth studying because deterrence is linked to entanglement and can cause deterrence failure and escalation to nuclear war.[33] The remainder of this section describes each of Narang's three postures and applies some considerations described previously to derive possible impacts of entanglement.

The first posture is a catalytic nuclear posture. This posture involves nations who leverage their small nuclear arsenals, or a latent breakout nuclear capability, as a means to garner support from a more powerful nuclear third state. The posture involves use of a coercive threat to the third state by threatening that as a weaker nation, if another regional power were to threaten it, they might be forced to use nuclear force, unless the third power was willing to step in and balance on its behalf. The third party benefits by stability in the region and in the case of latent nuclear powers, prevention of proliferation to the catalytic state.[34] For this entanglement discussion, states that pursue a catalytic posture with only a latent capability is not relevant. However, those using this posture with fielded nuclear forces are.

For nuclear states involved in a catalytic posture, there are two relevant unintended escalation possibilities due to entanglement considerations. These are the degree of entanglement of the catalytic state's nuclear arsenal and the degree of entanglement of the competing regional power's nuclear arsenal. For the third-party state, inherent in this posture is the idea of alliance, which entails a risk. If conflict were to occur, the third party could be drawn into the conflict via mutual security guarantee. Understanding that an alliance agreement could draw it into a conflict between two nuclear-armed states, the third party would need to make known and unknown entanglement risk calculations for both the potential aggressor state and the catalyst state, to understand if maintaining conventional conflict is a viable course of action if a crisis unfolds in the region.

It begins with the degree of entanglement of the regional competitor the catalyst state is trying to balance against. Depending on the degree of entanglement of the regional competitor, a third party may seek to change the catalyst arrangement. If the opponents' systems are greatly entangled, the third-party state may perceive providing support to the threatened regional ally to be too risky to pursue. In addition, if the threatening regional power makes the same calculation and concludes the third-party state is unlikely to risk conventional attack due to entanglement on behalf of the catalyst state, the third party's ability to support the threatened catalyst state with other instruments of national power would also be diminished. Once conventional military action is seen as not credible, the military instrument of national power would be less effective in supporting a third party's diplomatic and economic efforts in the region. Thus, the effectiveness of this posture for a catalyst state and its third-party protector against a competing regional power is reduced by entanglement.

Nearly the same factors are present if the catalyst state is a nuclear state whose systems are entangled. Because this posture depends on some degree of coercion of the more powerful third party to assist on the regional power's behalf because of some benefit, or more likely absence of a bad outcome for the third party in the event of a regional conflict, entanglement effects this relationship by forcing

the third party to evaluate the likelihood of escalation during a crisis. The third party needs to evaluate the extent to which the regional power's nuclear systems are entangled and its effects on stabilization during a crisis. A third party might be less likely to intercede, if the escalation risks in its view is already too great due to entanglement and the third party doesn't believe it could stabilize the situation.

However, there may be benefits for entanglement for the catalyst state. If a regional power believes conventional attack on a catalyst state is unlikely to remain conventional, the catalyst state may be able to deter conventional levels of violence without the third party's security guarantees via entanglement.

The second posture involves assured retaliation. In this posture, nuclear states use the assured threat of nuclear response only after an actual nuclear attack to deter nuclear aggression.[35] In this case, entanglement tripwires and brinkmanship discussed above would be less applicable because the state is committed to absorbing a nuclear attack prior to response. Thus, a conventional attack on dual-use systems would not be as likely to escalate until an actual attack with nuclear weapons is used. Additionally, because a state pursuing this posture would not attack first, entanglement of an adversary's system is also less relevant. It is true a state's pursuing an assured response posture could lower the threshold for escalation through entanglement. However, in doing so it would no longer be using an assured retaliation posture, but would more closely reflect Narang's third posture, an asymmetric retaliation posture.

The third posture utilized by regional nuclear powers is asymmetric escalation. This posture requires a state's ability to respond to a conventional attack with a fast nuclear response. The posture requires nuclear forces to maintain a higher state of readiness than other postures to maintain credibility that nuclear weapons are available and ready to be used in a response to an attack. Narang alludes to entanglement as a means to achieve deterrent credibility noting, "To achieve credibility, asymmetric escalators must be transparent about their capabilities, deployment patterns, and broad conditions of use, requirements that can generate significant command and control pressures and increase the risk of inadvertent use of nuclear weapons."[36]

From an entanglement standpoint, states using this posture increase their nuclear deterrent's credibility through both unknown and known entanglement risks. During a crisis, but prior to actual violence, the aggressive posture of the asymmetric escalator's nuclear forces to provide reaction to attack provides credibility, but also increases the likelihood the state could misinterpret an adversary's act as a prelude to attack or actual attack.

On the opposite side, a state attacking an asymmetric escalator state will likely be less concerned about entanglement risks of conventional attack, because of the asymmetric escalator's extremely low threshold for nuclear response. In other words, the asymmetric escalator is postured to escalate against an attacker even in early stages of conflict and at low levels of violence. In most cases, it is unlikely an attacker seeking military gains, could maintain an attack below a level of violence, to which the asymmetric escalator would not escalate to nuclear conflict.

Further, entanglement risks of an aggressor to an asymmetric escalator may also be amplified. For example, an asymmetric escalation state may adopt a launch on warning doctrine. Such a doctrine increases risks that during a conflict any missile launch by an attacking state with dual-use missiles would likely garner a nuclear response from the asymmetric escalator even before the nature of the attack is confirmed to be nuclear.[37]

Entanglement and the Stability Instability Paradox

The stability instability paradox posits that nations with nuclear weapons are more stable because large total wars will be unlikely and yet less stable because lower levels of conflict are more likely. On the stability side of the theory, nuclear states will avoid total war conflicts with each other because of the threat that an attack on a nuclear-armed state's homeland would garner a certain nuclear response. However, the certainty of nuclear response also leads to instability. Because an attack on a homeland is untenable, the risks of war are reduced because the state losing the conflict does not risk occupation of the homeland or regime change, both of which are more likely if a nonnuclear state loses a conflict.[38] Further, the costs of waging war are reduced, making lower levels of conflict more likely. In this case, the costs are reduced because occupation of another state's homeland is not an option. Therefore, the associated costs in blood and treasure of total war victory are not incurred. Pulling from the bargaining theory of war, the astronomical increase in risks to total war balanced against the much-reduced costs of limited war yields a great likelihood of limited small wars between nuclear states.[39]

The paradox provides interesting context to consider entanglement and, on its surface, illustrates that entanglement perhaps is not a major factor in the interaction and relationships of nuclear states. However, this is incorrect. Taking the stability half of the paradox first, it is unlikely any nuclear state would allow a conventional attack on its homeland to the point that the regime or state's existence is threatened and not use its nuclear weapons. For states with a stated posture of asymmetric escalation, the stability half of the paradox is without question valid. However, even for states employing a no-first-use doctrine, the idea of using nuclear weapons as a last resort to avoid occupation, seams all too likely and thus suggests nuclear states will avoid major levels of violence against each other. Posen states this idea is both widely accepted and also easy for politicians to anticipate and to develop plans.[40] Civilian leaders are unlikely to challenge nuclear states purposely and directly because of the near certainty of the enormous costs involved.

The second half of the paradox that lower levels of conflict are more likely, seems to be in conflict with the ideas of entanglement and their dangers for escalation. However, at the very center of the paradox argument is the idea that a threshold would not be crossed by nuclear states in a limited war. Further, the entanglement escalation argument posits that thresholds are not always obvious to both belligerents. Glenn H. Snyder alludes to this when he states a counter argument to the instability side of his argument saying, "But one could argue precisely the opposite – that the greater likelihood of gradual escalation due to a stable strategic

equilibrium tends to deter both conventional provocation and tactical nuclear strikes – thus stabilizing the overall balance."[41] Thus, the paradox and the entanglement arguments operate on shared reasoning. The paradox requires thresholds be known, when they are unknown due to the entanglement, the paradox is invalid. The paradox predicts behavior and is more applicable in an environment of obvious thresholds between belligerents. The escalation model can account for situations where thresholds are vague and not clearly understood via brinksmanship.

A second consideration in the interaction between the stability instability model and escalation via entanglement is that states that are conventionally weaker and vulnerable to conventional attack could seek to lower the nuclear threshold via entanglement. Using India and Pakistan as examples, the stability instability model would predict Pakistan will be vulnerable to limited attack from India at a level of violence below the nuclear threshold because Pakistan is conventionally weaker.[42] However, in this case, Pakistan could reduce controls on nuclear weapons or field tactical nuclear weapons closer to its boarders using entanglement brinksmanship to lower the nuclear threshold specifically against India's conventional superiority. Thus, Pakistan could inject instability via entanglement in its nuclear balance with India to deter conventional aggression.

Conclusions

The discussion above attempts to highlight under what conditions escalation entanglement risks will generally increase or decrease considering classic deterrence theory, current entanglement literature and contemporary entanglement issues. Entanglement risks will change based on many factors, most notably the credibility that the entangled system, if targeted, will critically degrade the nuclear deterrent. Further, credibility that targeting a state's entangled systems would be escalatory, is affected by the size of a state's nuclear arsenal and its nuclear posture. Finally, the stability instability paradox supports the entanglement theory presented here because entanglement moves the nuclear threshold without challenging or altering the overall basis of the paradox theory.

Based on the analysis above, it is likely entanglement could be beneficial to states with small nuclear arsenals with limited conventional capabilities. As Acton points out, while many of China's systems, particularly its NC3, are highly entangled with its conventional systems, there is no evidence to support the entanglement is purposeful.[43] This paper doesn't attempt to prove otherwise, but does suggest nuclear nations, particularly non-superpower (regional nuclear power) states could use entanglement in the future to raise the level of risk associated with a conventional attack against their interests. Intentional or not, there are several benefits states may attempt to capitalize on. As discussed above, entanglement has an ability to raise the potential costs of conventional war by introducing a threat of unintended escalation to nuclear conflict. The increased risks of unintended consequences take two forms – known risks via tripwires and unknown threats causing brinkmanship. For states that are vastly outmatched conventionally, raising the cost of conventional war is in effect deterring conventional conflict by using

their nuclear deterrent. The idea of intentional entanglement would be most effective for states using an asymmetric escalator posture because the posture reinforces credibility that targeting entangled risks within their strategic deterrent is escalatory. Similarly, superpowers will seek to mitigate entanglement risks to both maintain a stable international environment, as well as a conventional military advantage.

Further adding to this argument is that technological advances make counterforce strikes against nuclear arsenals more viable. Because the existing nuclear arsenals are at increased risk of attack, attacking dual-use systems, even support systems such as command and control, is more escalatory than if a counterforce attack was not viable. Further, increased dependency of space and cyberspace exacerbate entanglement risks because of the increased complexity and speed of operations within these domains. Further, cyber collateral damage increases risks of inadvertent entanglement because dual-use systems could be accidentally targeted via cyberattack.[44] Finally, there is a possibility that an adversary could misunderstand cybersurveillance software as cyberattack software. If this code was thought to be targeting a dual-use system, this would be very escalatory.[45] These factors increase the likelihood that a state that pursues intentional entanglement to deter conventional attack would have credibility.

While it is clear in some instances, states will derive a deterrent benefit through entanglement, military planners need to do more analysis on specific adversaries and situations to better understand the interaction of variables like forces size, posture, doctrine, weapons, and their interaction with entanglement. This paper concludes that states with small nuclear forces with a perceived conventional imbalance with a regional competitor are most likely to purposely entangle to deter conventional aggression. Further, states using an asymmetric escalation posture will most directly derive benefit of purposeful entanglement.

Policy Implications and Mitigation Measures

First, the U.S. policy should understand entanglement will be adventitious to some states in certain instances because it degrades a U.S. conventional advantage. One challenge for American planners going forward is to understand the posture of a state. Nuclear posture is not static and could change over time. American planners need to understand if a state is committed to an assured response posture or under what circumstances the state might become an asymmetric escalator. China, for example is sending mixed signals. On the one hand, the Chinese ascribe to a no-first-use policy that is indicative of an assured response posture. On the other hand, its arsenal is growing in numbers, complexity, and capability, while its strategic and conventional systems are becoming more entangled. American policymakers should wonder if China's entanglement might someday soon become a deterrent from conventional attack until China reaches conventional parity with the United States.

Therefor the United States should seek to minimize entanglement risks wherever possible. One avenue to reduce entanglement risks is by developing norms for cyber. Additionally, space norms should be further developed. This is an

expansion of policies developed early in the Cold War when the United States and the Soviet Union recognized the strategic importance of space in future conflicts. The Outer Space Treaty ensured that nuclear weapons would not be deployed to space or on celestial bodies. Further because space-based satellites were used for early warning of an ICBM attack and treaty verification, they were protected under the Anti-Ballistic Missile Treaty (ABM Treaty or ABM). If either nation targeted these systems, the other would likely assume a full-scale nuclear attack via ICBM was immanent, which could lead to a preemptive attack by the other side. For this reason, through the Outer Space Treaty and ABM both the United States and the Soviet Union largely limited their abilities to target each nations' strategic space assets.[46] The transparency offered by these now outdated agreements ensured avoiding inadvertent entanglement via space-based early warning systems and should be revisited to account for modern systems.[47]

Secondly, nuclear nations should develop and advocate policies that limit launch-on-warning policies. The cyber nuclear weapons study group recommends "developing options to increase decision time to account for cyberthreats to early warning systems."[48] The United States should advocate for an agreement among nuclear nations to adopt a doctrine that decreases launch on warning because of potential vulnerabilities of cyberattack on NC3 by nonstate actors. Limiting launch-on-warning doctrine would limit the impact of a nonstate spoofing attack by easing time constraints of decision makers to appropriately attribute the source of the attack and thereby limiting the threat of escalation. Further, some nuclear nations use the same delivery systems for both conventional and nuclear weapons, that early warning systems cannot differentiate. A decision to retaliate with a nuclear response prior to detonation, could prove premature if the weapons carry only a conventional payload.

Additionally, drawing from another Cold War example, in 1963 just a few months after the Cuban Missile Crisis, a Memorandum of Understanding created a direct communication link or "hotline" between the United States and Soviet Union. The hotline offered fast and easy communications between both Washington and Moscow during times of increased tensions in order to avoid inadvertent nuclear war. Many states, including Russia, China, India, and Pakistan, deploy these lines today, which have been effective during a crisis.[49] However, they are less likely to be effective once actual combat begins because diplomacy will be reduced. Perhaps the most optimistic of all recommendations put forth here, considering modern entanglement risks, this diplomatic norm should be challenged. Because the body of nuclear deterrence theory posits the primary function of nuclear arsenals are as insurance that an adversary won't use its nuclear weapons because of the undesirable likelihood that a devastating counterattack would occur, it is unlikely any nuclear nation seeks nuclear conflict, even during conventional conflict. Therefore, both sides should maintain robust communications even during conventional war. One possibility would be through a pre-identified third-party interloper and real-time around the clock interaction of each side. The two states in conflict should maintain constructive and frank dialog during conventional conflict specifically to address entanglement and escalation risks. While deterrence may have failed to avoid a conventional war, there is a strong likelihood that neither side

favors escalation to nuclear war. A third party could provide a ready avenue to air misunderstandings related to targeting of entangled dual-use systems during conventional conflict between nuclear-armed adversaries.

Finally, there are several things the United States could pursue on its own to mitigate risk of U.S. actions would unnecessarily escalate a limited conventional conflict to nuclear war. First is to consider what changes to the National Combatant Command Structure are needed to allow a conventional war to be informed by escalation risks. Currently conventional attacks by the geographic commander could complicate the U.S. Strategic Command (USSTRATCOM) mission of deterring strategic attack by threatening the adversary's nuclear deterrent.[50] More study needs to be done in this area as current doctrine does not fully address these potential conflicts in assigned mission roles. U.S. doctrine needs to evolve beyond conventional war winning against a nonnuclear state, to address conventional war winning while maintaining nuclear stability versus nuclear-armed near-peer states.

Secondly, James Acton recommends that U.S. officials develop an understanding of entanglement risks and appoint one official to ensure entanglement considerations are integrated into acquisitions of NC3, war planning and other aspects of the U.S. military.[51] Drawing from this idea, one option could be providing this responsibility to the USSTRATCOM commander. There is some precedence for assigning such broad authorities and responsibilities to one combatant commander over others. One example, in August 2018, U.S. Secretary of Defense James Mattis assigned the USSTRATCOM commander responsibility to oversee all aspects of NC3 including "operations, requirements, systems engineering and integration."[52]

Additionally, policymakers and military advisors need to be honest and frank about the increased costs of pursuing a conventional conflict where entanglement risks are present. Timelines and risks to American military members might be purposely increased to avoid entanglement escalation. Talmadge provides an example of a U.S. conventional conflict with China where U.S. commanders may need to accept a risk from conventionally-armed Chinese mobile missiles, because attacking Chinese mobile missile C3 would be detrimental to China's nuclear deterrent and therefore very escalatory.[53] James Acton advocates that the prioritizing avoiding escalation over conventional warfighting goals, arguing that a stated goal of any operations plan must be to maintain the level of conflict below the nuclear threshold, paying special attention to the specific entanglement threats of the crisis.[54]

This paper has argued that deterrence theory suggests that because technological advancements have made nuclear arsenals more vulnerable to counterforce attack and entanglement more likely, in some cases, a state's nuclear posture, its arsenal size and composition could make purposeful entanglement a credible deterrent against conventional attacks. The paper finds that specific nuclear postures and nuclear arsenal sizes make intentional entanglement a credible option for some nations to deter conventional attack. The paper also provided recommendations to U.S. policymakers to help them both understand and reduce entanglement escalation risks.

Chapter 3 Notes

1. William Burr and Thomas Blanton, *The Submarines of October, US and Soviet Naval Encounters During the Cuban Missile Crisis* (Washington D.C.: National Security Archive Electronics Briefing Book No. 75, 2002), George Washington University, accessed Jan. 20, 2019, at https://nsarchive2.gwu.edu/NSAEBB/NSAEBB75.

2. Barry Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, N.Y.: Cornell University Press, 1991), p. 3.

3. Keir A. Lieber and Darryl G. Press, "The New Era of Counter-Force: Technological Change and the Future of Nuclear Deterrence," *International Security*, vol. 41, no. 4 (Spring 2017), p: 9-12.

4. Ibid. pps. 9-12, 46-48.

5. Ibid. pps. 9-12, 23.

6. James M. Acton, "Escalation Through Entanglement," *International Security*, vol. 43, no. 1 (Summer, 2018), p. 74.

7. Lieber and Press, "The New Era of Counterforce," p. 10.

8. U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," Defense Science Board, Washington, D.C., January 2013), p. 21, accessed at www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf.

9. Stoutland et al., "Nuclear Weapons in the New Cyber Age," The Cyber-Nuclear Weapons Study Group, September 2018, p. 7, accessed June 4, 2019, at www.nti.org/analysis/reports/nuclear-weapons-cyber-age/.

10. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, D.C.: Department of Defense, January 2013), p. 21, accessed at www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf.

11. Stoutland et al., "Nuclear Weapons in the New Cyber Age," pps. 15 and 21.

12. Todd Harrison, Kaitlyn Johnson, and Thomas G Roberts, "Space Threat Assessment 2018, CSIS Aerospace Security Project 1-3, accessed at www.csis.org/analysis/space-threat-assessment-2018.

13. Acton, "Escalation Through Entanglement," p. 62.

14. Shirley Khan, "China's Anti-Satellite Weapons Test," CRS Report, Chinese ASAT Test Report, April. 23, 2007, p. 2

15. Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press, 1966), p. 47.

16. Acton, "Escalation Through Entanglement," pps. 56 and 84-85.

17. Ibid. pps. 66-68.

18. Thomas Schelling, *The Strategy of Conflict* (Cambridge, Mass.: Harvard University Press, 1960) p. 6.

19. Acton, "Escalation Through Entanglement," p. 62.

20. Carin Zissis, "China's Anti-Satellite Test," Council on Foreign Relations, Feb. 22, 2007, accessed Feb. 26, 2019, at www.cfr.org/backgrounder/chinas-anti-satellite-test.

21. Office of the Secretary of Defense, *Nuclear Posture Review* (Washington, D.C.: Department of Defense, Feb. 21, 2018), p. 21

22. Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press, 1966), pps. 99-105.

23. Caitlin Talmadge, "Beijing's nuclear option: Why a U.S.-Chinese war could spiral out of control," *Foreign Affairs*, no 97, (2018), p. 2, accessed at https://search-proquest-com.aufric.idm.oclc.org/docview/2129468596?accountid=4332&rfr_id=info%3Axri%2Fsid%3Aprimo.

24. Office of the Joint Staff, J7 (Force Development), *Cross-Domain Synergy in Joint Operations, Planner's Guide* (Washington, D.C.: Department of Defense, Jan. 14, 2016), pps. 50-52, accessed at www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230.

25. Patricia M. Kim, "Chinese Perceptions on Nuclear Weapons, Arms Control and Nonproliferation," prepared statement for Subcommittee on Terrorism, Nonproliferation, and Trade, U.S. House Foreign Affairs Committee, U.S. House of Representatives 2nd Session, 115th Congress, June 21, 2018, pps. 2-5, accessed Jan. 9, 2019, at https://docs.house.gov/meetings/FA/FA18/20180621/108459/HHRG-115-FA18-Wstate-KimP-20180621.pdf.

26. Posen, *Inadvertent Escalation*, p. 3.

27. Ibid. p. 20.

28. Vipin Narang, *Nuclear Strategy in the Modern Era, Regional Powers and International Conflict* (Princeton, N.J.: Princeton University Press, 2014), p. 14.

29. Posen, *Inadvertent Escalation*, p. 2.

30. Lieber and Press, "The New Era of Counterforce," p. 10.

31. Ibid. p. 12

32. Lieber and Press, "The New Era of Counterforce," p. 12.

33. Narang, *Nuclear Strategy in the Modern Era*, pps. 14-23

34. Ibid. pps. 15-16.

35. Ibid. pps. 17.

36. Ibid. pps. 19.

37. Stoutland et al., "Nuclear Weapons in the New Cyber Age," p. 8.

38. Glenn H. Snyder, "The Balance of Power and the Balance of Terror," in Paul Seabury's *Balance of Power* (San Francisco, Calif.: Chandler Publishing Company 1965), p. 186-200.

39. William Spaniel, "The Stability-Instability Paradox," (video), *International Relations* 101 (#66), accessed at www.youtube.com/watch?list=PLB5965C13F4B0B2DA&time_continue=7&v=MFLxlc61xJY

40. Posen, *Inadvertent Escalation*, pps. 1-2.

41. Snyder, "The Balance of Power and the Balance of Terror," p. 199.

42. Zulfqar Khan and Rubina Waseem, "South Asian Strategic Paradox: India-Pakistan Nuclear Flux," *Journal of Strategic Studies*, no. 35 (2015), p. 7.

43. James Acton, "Escalation Through Entanglement," Carnegie Live, Sept. 12, 2018, accessed Jan. 19, 2019, at www.youtube.com/watch?v=iex594MHEQQ.

44. Corey Hirsch, "Collateral Damage Outcomes are Prominent in Cyber Warfare, Despite Targeting," International Conference on Cyber Warfare and Security, (2018) pps. 282-283, accessed at https://search.proquest.com/openview/12cbf1c24ddb996facc738940d60a7df/1?pq-origsite=gscholar&cbl=396500

45. Acton, "Escalation Through Entanglement," p. 92.

46. "The Anti-Ballistic Missile Treaty at a Glance," Arms Control Association, Washington, D.C., August 2012, accessed Jan. 26, 2018 at www.armscontrol.org/factsheets/abmtreaty.

47. Alex B. Englehart, "Common Ground in the Sky: Extending the 1967 Outer Space Treaty to Reconcile U.S. and Chinese Security Interests, *Pacific Rim Law & Policy Journal*, (2008), p. 145-150, accessed Jan. 21, 2018, at https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/568/17PacRimLPolyJ133.pdf?sequence=1.

48. Stoutland et al., "Nuclear Weapons in the New Cyber Age," p. 8.

49. "Hotline Agreements and Fact Sheets," Arms Control Association, Washington, D.C., April 2018, p. 1, accessed Jan. 15, 2019, at www.armscontrol.org/factsheets/Hotlines.

50. *Department of Defense Joint Publication 1* (Washington, D.C.: U.S. Department of Defense, March 25, 2013, Change 1 incorporated July 12, 2017), p. XVII, accessed at www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

5. James Acton, "Escalation Through Entanglement," Carnegie Live, Sept. 12, 2018, accessed Jan. 19, 2019, at www.youtube.com/watch?v=iex594MHEQQ.

52. Sandra Erwin, "US STRATCOM To Take Over Responsibility for Nuclear Command and Control, *Space News*, July 23, 2018, accessed Jan. 30, 2019, at https://spacenews.com/u-s-stratcom-to-take-over-responsibility-for-nuclear-command-control-and-communications.

53. Talmadge, "Beijing's nuclear option, p. 3-4.

54. James Acton, "Escalation Through Entanglement," Carnegie Live, Sept. 12, 2018, accessed Jan. 19, 2019, at www.youtube.com/watch?v=iex594MHEQQ.

CHAPTER 4

Don't Be Caught in the Dark: Examining Deterrence Options for a High-Altitude Electromagnetic Pulse Limited Nuclear Attack

Dr. Lyndon "Kyle" McKown, U.S. Air Force

> *"The electromagnetic pulse (EMP) generated by a high-altitude nuclear explosion is one of a small number of threats that can hold society at risk of catastrophic consequences …. A single EMP attack can seriously degrade or shut down a large part of the electric grid in the geographic area of the EMP exposure effective instantaneously. There is also the possibility of functional collapse of grids beyond the exposed one, as electrical effects propagate from one region to another …. Should significant parts of the electric infrastructure be lost for any substantial part of the time, the Commission believes that the consequences are likely to be catastrophic, and many people will ultimately die for lack of the basic elements necessary to sustain life in dense urban and suburban communities."*
>
> – 2008 Report of the Commission to Assess the Threat to the United States from EMP Attack[1]

One Second After, an unsettling novel by award-winning author William R. Forstchen, details how an attack on the U.S. homeland using a nuclear EMP instantaneously transforms this country from the digital age back to the turn of the 20th century.[2] In this doomsday scenario, the United States is literally left in the dark, with no electricity, no electronic technology, and a collapsed civilian infrastructure. The results are catastrophic and over the next year 90 percent of the population perish from the lack of medical care, starvation, and civil unrest. While the likelihood of any nuclear attack is considered low, the consequences are so high that for many years the U.S. military establishment has been conducting research and taking concrete actions to ensure they are ready for just such an attack.

The problem is, that unfortunately, our government has only recently started to evaluate the potential effects and needed preparations for the civilian infrastructure to survive an EMP attack. While a start, this governmental effort is still fragmented across multiple agencies and unduly handicapped because of the current classification of relevant government research data. All of which has led to a failure to set and implement industry standards to protect the civilian infrastructure from the most potent of the EMP threats. To correct this potentially catastrophic vulnerability and avoid the "One Second After" doomsday scenario, stronger governmental leadership, improved transparency, and industry-wide federal standards are needed to send a strong signal of preparedness and resilience to deter any potential aggressors.

This research will explore the U.S. vulnerability to an EMP attack and seek a deterrent solution that may also address a recent Headquarters U.S. Air Force/A10 question of interest:

> *In this era of great power competition, how do adversaries perceive the U.S. nuclear posture or policy and their impact on strategic stability?*[3]

The background for this question talks about deterrence as a function of capability, credibility, and national will or intent. It also questions whether adversaries are most intimidated by mass, technology, or policy (such as preemption, first strike use, and posturing forces). This background information appears to focus on a type of deterrence referred to as deterrence by punishment. This is problematic because many experts have expressed concern that in the arena of limited nuclear warfare between great powers, and even more so with lessor or nonstate aggressors, deterrence by punishment may be difficult to execute and/or less effective than deterrence by denial or a combination of broader tailored deterrence approaches.[4] My research will examine this concern, look at the deterrence options against this type of threat and suggest policy recommendations designed to reduce the probability and consequences of such an EMP attack.

Research Question and Thesis

As suggested in the introduction, the scope of this research is bounded to looking only at limited nuclear warfare. Additionally, based on my initial literature review and the numerous aspects and possible capabilities and tactics associated with limited nuclear warfare, this research will focus specifically on how best to deter a limited nuclear attack on the continental United States via a high altitude EMP. Specifically, this research will attempt to answer the question:

> *What is the best method of deterrence for a limited nuclear attack via a high-altitude electromagnetic pulse, deterrence by punishment or deterrence by denial?*

My hypothesis is an adversaries' perception of the United States as being unprepared for attack greatly increases the likelihood of the attack. Without improved resiliency of our civilian infrastructure (primarily the power grid and communications), pure deterrence by punishment may fail because aggressors will likely conclude a high probability of achieving the negative effects they desire and take their chances on any retaliatory response. Additionally, the aggressor may also doubt the credibility of a U.S. threat to respond to an EMP attack with nuclear weapons and may not sufficiently fear a conventional response enough for deterrence by punishment to be effective. Therefore, deterrence by denial would be the best method of deterrence against an EMP attack against the United States. At the very least it would seem prudent to attempt to utilize some combination of punishment and denial to increase the deterrent and other positive effects and in turn the strategic stability. While the scope of this effort was narrowed significantly because of the limited amount of time to complete the research, the results may have broader implications to deterrence theory in general.

Definition of Terms

Deterrence

Deterrence is an ancient concept, the Roman adage "if you want peace, make ready for war" clearly illustrates this point.[5] A more modern definition is found in the Oxford dictionary and states, "The action of discouraging an action or event through instilling fear or doubt of the consequences." There are two basic approaches to deterrence – deterrence by punishment and deterrence by denial.[6] Both approaches are fundamentally psychological and entail the nuanced shaping of perceptions in the mind of the potential aggressor. In other words, we seek to get inside an aggressor's head and manipulate the decision making in ways that restrain the aggressor from taking the undesired action. This manipulation is possible due to the rational adaptation to the deterrence approaches designed to change its cost-benefit calculus.

Deterrence by punishment approaches are essentially designed to affect the perceived costs associated with an action. This approach threatens to inflict severe penalties as punishment in response to an action. To be most effective, the threat of punishment must come from someone who has the capability, the credibility, and the will to use it, should it be needed. It is also most effective if the punishment is swift, certain, and severe.

Conversely, deterrence by denial, is a form of deterrence where an action is discouraged because the expected benefit of the attack is negated or the potential success rate appears too low. For example, defensive measures to hold off an incoming attack or increased resilience that limits damage would be considered to reduce the perceived benefits in the mind of the aggressor and thus its likelihood of an attack.

While the concept of deterrence is as old as war, the advent of nuclear weapons was the catalyst that brought the logic of deterrence under the microscopic scholarship of international relations.[7] Since this time, there have been multiple waves of nuclear deterrence theory evolution as the concept evolved in response to

the environment in which it operated. Bernard Brodie led the first wave using deductive theory and theoretical strategizing. Thomas Schelling and Herman Kahn applied tools like game theory to develop the conventional wisdom in the second wave. During this period, the deterrence by punishment approach was firmly established by Schelling, while Kahn's advocacy for a broader approach to deterrence to include defensive activities was largely ignored until most recently. The third wave was characterized by the use of statistical and case study methods to test second wave theory and challenge the rational actor model assumption.

Finally, while the first three waves were developed primarily in the Cold War security environment, current fourth wave authors analyze deterrence in a post-9/11 security environment. This post-Cold War change in the security environment context and its effect on the validity of some of deterrence theory's conventional wisdom assumptions is a central aspect of this research and deserves additional attention.

Thomas Schelling was a Nobel Laureate who used the "rational actor" model of modern economics to develop the punishment approach to deterrence. Schelling recognized that with nuclear weapons, military victory was no longer the "price of admission" for the ability to successfully employ the threat of violence. He asserted, "Deterrence rests today on the threat of pain and extinction, not just on military defeat."[8] His philosophical belief was that actual nuclear warfare was unthinkable and therefore he supported an approach of a balance of terror based upon mutual vulnerability. A strategy of assured destruction and later mutually assured destruction (MAD) was officially adopted by the United States for much of the Cold War based on this approach.[9] His approach called for minimum deterrence that required only the minimum number of weapons necessary to unleash an unacceptable level of destruction upon the Soviet Union's infrastructure and civilian population. He advocated maintaining similar force structures to help make the terror "stable." Conversely, anything such as civil or missile defenses designed to reduce vulnerabilities and protect human resources was seen by Schelling as inherently destabilizing. Schelling's approach of deterrence by punishment, was in effect, each side holding the other's civilian populations as hostages.

Herman Kahn's philosophical views differed from Schelling's. First, Kahn cast doubt on the widely accepted theory of a mutual balance of terror. He argued that in order to achieve success the terror had to be mutual and reliable. What if one side thought that, given sufficient preparations, although difficult, they could prevail in a nuclear war? He feared this could result in another Pearl Harbor for the United States. Another stark difference was while Schelling viewed reducing vulnerabilities and seeking superiority as destabilizing, Kahn favored seeking to limit damage through defensive measures and strategic superiority through an array of offensive capability as more effective and safe deterrents. In taking this approach Herman Kahn was adding "deterrence by denial" to Schelling's "deterrence by punishment." Even though this approach seems more robust than Schelling's, addressing both a potential adversaries' perception of the cost and benefits in their decision calculus, Kahn was largely ignored until recently.

One of the reasons that Schelling's deterrence by punishment was so strongly endorsed during the Cold War was that most experts and leadership felt

that defending against total war involving nuclear weapons was nearly impossible. They felt that a total nuclear war simply could not be won and therefore must never be fought. Additionally, they assumed that the Soviets shared this same outlook on total war, because anything otherwise would not be rational. The strategy on both sides during the Cold War was the nuclear threat had to be always ready and credible, but never used because a nuclear war could not be won. While these assumptions may have been valid in the past, there is growing evidence our adversaries' strategies may be changing and we must begin to start dealing with some new realities.

Limited Nuclear War

One of these new realties is that the long-held proposition, nuclear wars cannot be won and therefore must not be fought, is fading in the eyes of our potential adversaries. Wes Mitchell in a recent article details how Russia's and China's new focus on "limited war" capabilities is challenging our traditional method of deterrence by punishment.[10] He asserts that there are at least three reasons for it getting harder to punish. First, the sheer number of competitors is increasing. Secondly, the rivals are becoming better armed. Finally, our rivals are developing new tactics designed to evade our retaliatory deterrence. His article is primarily focused on new tactics that try to operate below the threshold of deterrence by punishment to create territorial *faits accomplis*.

John Warden in another article describes similar disturbing trends providing additional evidence that leads one to have little doubt that our adversaries have formulated a new strategy, namely that nuclear wars can be won because they can be kept limited.[11] One envisioned scenario would be to capitalize on a surprise use of limited nuclear assets to quickly achieve an operational advantage and making it appear too costly for the United States to intervene because of the threat of escalation. This would be in effect an attempt to decouple theater and strategic warfare and challenge the resolve of our extended deterrence.

Another more subtle limited nuclear warfare trend described by Warden, most relevant to this research, is the attempt by adversaries to "distinguish between nuclear use consistent with Law of Armed Conflict traditions and strikes that are far less discriminating." This approach would be to use nuclear weapons in a way that causes few if any immediate civilian casualties and in doing so hope to avoid the backlash of transgressing the nuclear taboo. An upper atmosphere nuclear detonation designed to generate an EMP effect is just such an example. The motivation for such an attack could be multifold. First, a direct nuclear attack on the United States would probably be seen as too escalatory, since the threat of a U.S. retaliation with nuclear weapons would be credible, as it was during the Cold War. However, a limited nuclear EMP attack, while still having the potential to damage and downgrade military operations and civilian infrastructure, could be seen as somewhat reasonable and restrained when compared with mutual assured destruction. Second, the situation could be further complicated because the technology needed for such an attack makes it the perfect asymmetrical threat for a limited nuclear power or a rogue nonstate actor with a low-yield nuclear device and

a modified Scud missile. Additionally, Warden asserts, "These vulnerabilities might encourage adversary nuclear use, on the belief that they provide an opportunity for significant disruption of U.S. and Allied operations."[12] He then advises that these vulnerabilities should be mitigated with increased operational resilience. Increased operational resilience requires a thorough understanding of the characteristics and potential effects of an EMP.

EMP Characteristics and Effects

Experts in this field specify an EMP is composed of three component pulses designated E1, E2, and E3.[13] The E1 pulse is an almost immediate, brief, and very intense pulse that can induce tremendously high voltages into electronic circuits destroying vital components. It is unique to a nuclear event, has no similar counterpart in nature, and the data on the effects are classified for the most part. The E2 pulse is intermediate in duration and has similar effects to that of a lightning strike. The E3 pulse is much slower and longer lasting with effects similar to that of a solar storm. From the effects of natural solar variation we can predict this E3 effect from an EMP would virtually eliminate the ability to use radio communications (other than line of sight) for an extended period of time because of the absorption of radio waves by the ionized D-layer of the ionosphere.[14] Although many of the particular details on the potential vulnerabilities to these effects are classified, we know they can be devastating.

Understanding the vulnerabilities in the critical civilian infrastructure from an EMP, specifically the power grid and communications is a central part of this research. A recent *Executive Report to Congress* asserted, "The critical national infrastructure in the United States faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, as well as from natural EMP from a solar superstorm."[15] This report goes into great detail about a possible high-altitude nuclear EMP attack that could suppress the U.S. national command authority's ability to respond and thus negate the deterrence value of assured nuclear retaliation. Additionally, because of the dependence of society on the electrical power system and its vulnerability, this EMP attack could also create long-term, catastrophic consequences for our civilian population. It is reasonable to assume that potential adversaries are also aware of these vulnerabilities and might estimate the benefit of exploiting them to be worth the potential cost of retaliation punishment.

The final part of this research literature review focused on understanding the capabilities, cost, and benefits of reducing vulnerabilities through various technical solutions designed to eliminate or mitigate the adverse EMP effects. There is a wealth of literature available in this area that provides relatively simple technical recommendations to improve resiliency to help prevent or mitigate the adverse EMP effects.[16] Additionally, these experts argue that the costs to address these vulnerabilities are quite modest relative to the potential costs of repairing the damage caused by an EMP. Understanding the capability and potential costs of a deterrence by denial strategy is an important consideration in a decision for implementation since we must also use this data in our own cost-benefit analysis.

The key takeaway here is that we have the technical capability to develop a very high-quality defense against this threat at a reasonable cost to implement.

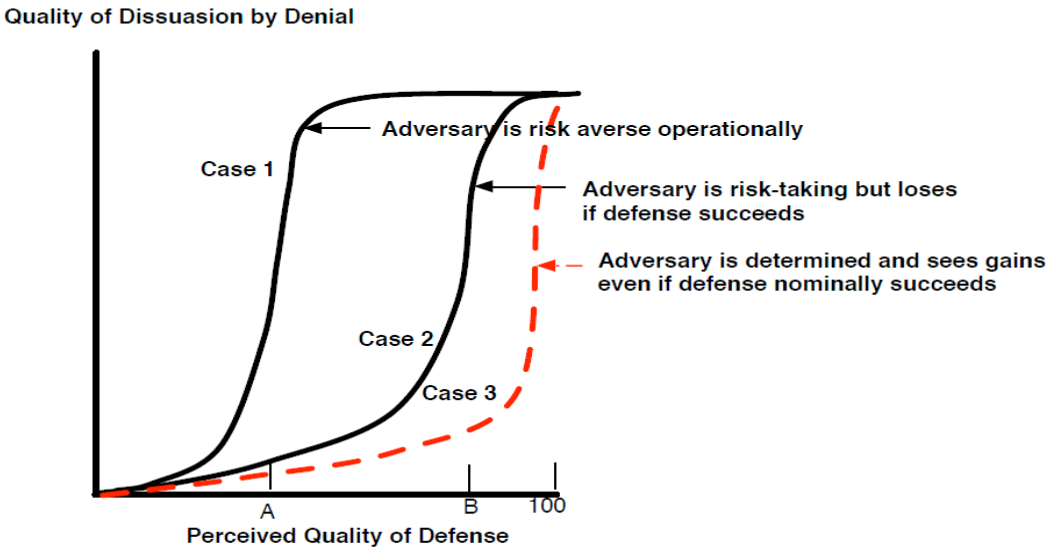
Methodology

In order to test my hypothesis, there needs to be some way to measure the effectiveness for deterrence by punishment and deterrence by denial and compare the results. Although a direct effectiveness measure would be desirable, measuring deterrence effectiveness quantitatively is problematic since this aspect is not understood very well nor has any direct measure been discovered in my literature review.[17] For this reason, a qualitative approach will be used by looking at the comparison utilizing a simple cognitive model proposed by Paul Davis in a RAND Corporation working paper in conjunction with an adaptation of standard cost and benefit analysis decision-making process.[18]

Davis begins his model development by redefining and relabeling Glenn H. Snyder's original deterrence by denial concept. Concerned that extending the definition of deterrence beyond its threat of punishment meaning confuses effective communication, he renames deterrence by denial to dissuasion by denial and proposes the following definition: "*Dissuasion by denial is deterring an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action."*

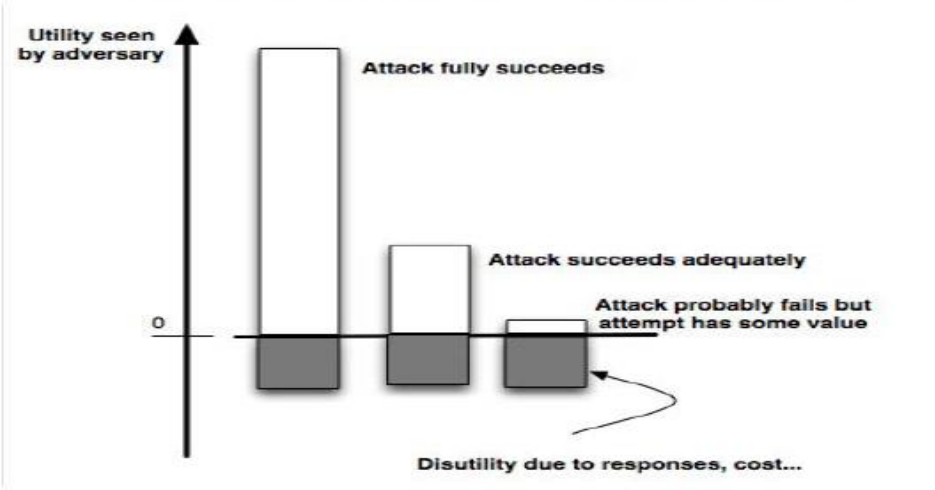
In examining his definition, it is clear that dissuasion by denial and defense are closely related. In fact, *Figure 1* depicts the quality of dissuasion by denial as a function of how good the defense is perceived to be by three notional cases of adversaries.

Figure 1 Actual and Perceived Quality of Defense



In Case 1, dissuasion by denial is very effective against an adversary that is operationally risk adverse and perceives the defense to be less than perfect, but sufficiently good. Case 2 depicts a more determined and risk-taking adversary that is only dissuaded if the defense is perceived as quite good. Case 3 depicts the most extreme adversaries that may see possible strategic gains even if the defense is near perfect and largely succeeds. In applying these concepts to the research question at hand, we can surmise that the effectiveness of deterrence by denial is directly related to how the adversary perceives the "Quality of Defense" against an EMP attack. Taking this to the extreme, it is arguable that if a perfect defense were possible and acknowledged by an adversary, deterrence by denial alone would suffice. In our particular case, while experts have provided ways to greatly reduce vulnerabilities and thereby increase the actual quality of defense against an EMP attack, there is no guarantee of an actual perfect defense. There is even less of a possibility that the adversary would perceive it as perfect. Therefore, it follows a comprehensive strategy should also include elements of deterrence by punishment that cause the adversary to evaluate the potential costs associated with an attack in comparison with the potential benefits in an adaptation of cost-benefit analysis as depicted in *Figure 2.*

Figure 2 Deterrence Depends on Both Positive and Negative Benefits



The basic framework for this approach rests on the rational actor assumption that we can take actions that manipulate the aggressor's decision making in ways that produce net security benefits. The manipulation is possible due to sensitivity and rational adaptation to operational risks posed by defensive measures that are designed to change the cost-benefit calculus. From a cost-benefit perspective, classic deterrence by punishment approaches are essentially designed to affect the perceived costs associated with an operation. Conversely, deterrence by denial, is where an operation is dissuaded because the adversary perceives the potential benefits appear too low. Since sensitivity and rational adaptation will vary depending on the type of potential aggressor and other unique situational factors, I will look at three general cases of potential aggressors: near peer, asymmetrical, and nonstate actor to using the methodology described above.

Each case will be analyzed in a notional scenario that portrays the situation in which the adversary could employ a limited nuclear EMP attack against the United States to achieve its political aims. While notional, each scenario will be based on reasonable expectations from current trends that could plausibly occur. The intent is heuristic rather than predictive with the intent of illustrating how a limited nuclear EMP might be used and serving as a venue to evaluate the two different approaches to nuclear deterrence in each case.[19] The answer to my research question will be surmised from analyzing the general results in how each one of these three types of aggressors might be affected in a decision to conduct an EMP attack against the United States.

Case Study Analysis

Near Peer

The apparent success of the U.S. Cold War nuclear deterrence strategy against the Soviet Union, namely deterrence by punishment, has served to reinforce the mainstream belief that the same basic approach will be sufficient in the current geopolitical situation. However, the United Sates is no longer in a bipolar environment, but now faces much more complex near-peer situations. Russia has nuclear parity with the United States and as detailed earlier, its military doctrine and exercises have increasingly embraced limited nuclear war capabilities and strategies. Similarly, an emerging China is challenging the United States economically, becoming increasingly capable militarily and aggressively pursuing new operational concepts such as unrestricted warfare.[20] Either country could be used in this first scenario, but I will use Russia because it still remains the only country with a nuclear arsenal capable of completely destroying the United States and thus would be our worst-case scenario.

In this scenario, we start with American and NATO troops in the Baltic countries and Russia's military buildup in neighboring Belarus making this region rife with tension and the stakes for conflict extremely high. Russia uses the excuse of protecting ethnic Russians as the rationale to invade one of the Baltic countries. NATO and Russian troops become embroiled in a conventional conflict that quickly escalates when Russia executes concerted conventional attacks against NATO bases and airfields in northern Europe, as well as a limited nuclear EMP attack against infrastructure and communication networks in Europe and the United States. Russia's limited nuclear EMP attacks are an attempt to incapacitate the United States and its allies temporarily to gain a regional tactical advantage in the Balkans. In this scenario the United States would have to balance the need to defend itself and allies against the possibility of further Russian escalation.

For this scenario, which deterrence option is best suited to counter such a limited nuclear EMP attack? Looking at the deterrence by punishment option, the 2018 *Nuclear Posture Review* provides U.S. declaratory policy regarding the potential employment of nuclear weapons:[21]

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 nonnuclear strategic

attacks. Significant nonnuclear strategic attacks include, but are not limited to, attacks on the United States, 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 nonnuclear weapons states that are party to the nuclear Non-Proliferation Treaty (NPT) and in compliance with their nuclear nonproliferation obligations. Given the potential of significant nonnuclear strategic attacks, the United States reserves the right to make any adjustment in the assurance that may be warranted by the evolution and proliferation of nonnuclear strategic attack technologies and U.S. capabilities to counter that threat.

In this scenario, while punishment is still possible, its deterrence effect has already failed. Russia has opted for such an attack because our infrastructure is currently vulnerable, our declaratory policy is vague, and they are gambling that the United States will limit or even preclude nuclear punishment in order to avoid possible escalation to total war. In other words, Russia has discounted the "fear of retaliation" costs by rationalizing the "fear of escalation" burden will mitigate or preclude punitive actions from the United States. This is certainly in line with Stephen J. Cimbala's concern that in many cases the idea of deterrence by punishment has become too risky because of the unpredictability of the nuclear escalation process.[22] Additionally, currently the United States would have few options for punishment beyond conventional weapons and yet short of strategic nuclear weapons because the number of nonstrategic nuclear warheads has declined by approximately 90 percent from September 1991 to September 2009.[23] The good news with a near-peer adversary is that because they have something to lose, punishment is possible, and in fact has to be applied if there is any hope of reestablishing this type of deterrence in the future. The major problem with the punishment approach is that it can only be demonstrated after it has already failed and in doing so there is a significant risk of escalation.

Turning to deterrence by denial, and referring to *Figure 1*, a near-peer adversary would probably fall into the Case 1 or Case 2 category, because of the risk of mutual destruction if the aggression led to total nuclear war. However, they might be tempted because our current situation of little to no defense is arguably increasing the probability of success of just such an attack. Supporting this line of thought, the *Executive Report to Congress* mentioned earlier concludes with this very powerful statement: "The consequence of continued failure to address the vulnerability of the United States to EMP generated by a high-altitude nuclear weapon invites such an attack."[24] Conversely, if we were to increase our infrastructure's resiliency even moderately, this could provide a very effective deterrence for a peer adversary effectively taking this limited nuclear option off the table. For limited nuclear war in general, many experts recommend a strategy of deterrence by denial, both as an end in itself and as a complement to deterrence by punishment. This approach presents both a strong defense that will deter low to moderate risk adverse opponents from believing that limited nuclear warfare will result in any benefit, and in the worst-case scenario still allow the option to impose punitive costs in the case that deterrence by denial fails.

For this scenario, I argue that deterrence by denial is preferable because putting up a strong and obvious defense sends a clear and unambiguous message to the peer aggressor that a limited nuclear EMP attack against the United States could not be effective. Therefore, there would be no benefit in this approach regardless of its calculus on the credibility of the punitive cost we would impose on them if they did attack in this manner.

Asymmetrical

We now shift from a focus on relatively symmetrical situations of mutual deterrence to what may be an even more complicated deterrence challenge from asymmetrical threats. For this case study we will analyze the following notional scenario with North Korea. Ongoing denuclearization talks between the United States and North Korea break down and economic sanctions continue to deprive Kim Jong-un of much needed hard currency. The United States obtains credible intelligence reports that North Korea has negotiated a deal to provide Iran with nuclear material and technology in exchange for oil and cash. Under the authority of a United Nations Security Council Resolution, the United States and its allies launch a maritime interdiction campaign against North Korean merchant ships believed to be carrying the materials. A North Korean ship is fired upon by the United States to disable it, boarded, and a load of centrifuges are discovered. In retaliation for the boarding, North Korea launches a nuclear EMP strike against the continental United States. Because of our current vulnerabilities, the strike is seen as the best use of its limited nuclear assets to cause the maximum damage to the United States.

In the case of an asymmetrical opponent, deterrence by punishment will continue to be an option, but in the case where the survival of the adversary state is in question, the adversary may feel they have nothing to lose. Nevertheless, in this particular scenario, there is little doubt punishment would be used as retaliation. The only question would be the conventional or nuclear nature of the response. However, since the threat of punishment diminishes because of desperation and the decision-making calculus shifts to the possibility of inflicting maximum damage as a last act of defiance, punishment's deterrence effect is questionable in this case. Alex S. Wilner supports this idea and further suggests that Cold War-style deterrence (deterrence by punishment) is not likely to be effective against potential aggressors from failing states or transnational groups.[26] So while punishment is always an option after the fact, why take the chance with this reactive and questionable approach when a more proactive approach is available.

From a deterrence by denial perspective, we again refer to *Figure 1*, where normally an asymmetrical adversary would probably fall into a Case 1 scenario because of its relative weakness compared to the United States. Therefore, they should be dissuaded from attack by a good defense. Even in the case of a failing state, a good to excellent defense and the associated low probability of success would arguably cause the adversary to rethink the situation and avoid the Case 3 scenario by attacking in some other way deemed more likely to succeed. In this notional scenario, North Korea decided to use an EMP attack on the United States

because of the perceived unaddressed infrastructure vulnerabilities and the possibility of putting the entire population in the dark. Under these circumstances, this would be a very effective use of its limited nuclear stockpile. However, addressing our infrastructure vulnerabilities and clearly communicating our defensive efforts would change the North Korean decision calculus. The North Koreans probably would not use their nuclear weapons for an EMP attack. Most likely, they would decide to attack in another way. What exactly that other attack mode or target will be is one of the central problems inherent in deterrence by denial. It is simply impossible to defend and deny every target. The best one can do is to defend the highest value targets and I assert that our civilian infrastructure should be designated and defended as such. Therefore, for my particular research question, I again argue that defense and deterrence by denial are the more effective approaches.

Nonstate Actor

Finally, turning to look at potential nonstate adversaries, especially terrorists, we will analyze the following notional scenario. The Islamic State of Iraq and the Levant (ISIL) is able to use propaganda to radicalize key personnel in a nuclear capable country and with their covert assistance steal a single nuclear weapon. In contemplating how to best use the weapon, they conclude that attempting to smuggle it into the United States for use is too risky. They decide to use a Scud missile fired from a shipping barge just off the coast of the United States to deliver the weapon. Additionally, they rationalize that while attacking a single city directly would inflict tremendous damage, using an air burst is more effective because it will devastate the entire electrical infrastructure of the continental United States because of its current extreme vulnerability. ISIL sleeper cells across the entire country will also be activated to take advantage of the resulting social unrest spreading the uncertainty and panic across the entire nation.

This analysis of deterrence against nonstate adversaries is the focus of the fourth wave of nuclear deterrence theory. Wilner and Jeffrey W. Knopf, two prominent fourth-wave scholars, discuss deterrence for these types of actors and while they both concur that deterrence is still applicable several aspects must be modified. Both agree that in this type of scenario, deterrence by punishment becomes much more problematic. First, nonstate actors and terrorists many times are more focused on the potential benefits of the operation than the costs. Additionally, if punishment is to be applied, there is also still considerable uncertainty about what kind of threatened response is most appropriate because deterrence by punishment requires knowing who the aggressors are and what they value in order to be effective.

Wilner argues that deterrence theory can still be applied to nonstate actors, but suggests a much broader definition of deterrence to include denial, defense, and mitigation. From this perspective, making preparations to manage the effects of an EMP attack is critical to reducing the potential benefits to bolster deterrence by denying the aggressors the desired negative effects they seek. From a deterrence by denial perspective, we again refer to *Figure 1*, where the nonstate adversary would

probably fall into a Case 1 or 2 scenario and be dissuaded from attack by a good to excellent defense. Since in this scenario, the nonstate actor only has a single nuclear weapon, deterrence by denial would be very powerful, because that actor would not want to waste its only weapon on an EMP attack that would have little effect. Even if the terrorists fall into a Case 3 scenario where they will carry out their attack in the face of a near perfect defense, deterrence by denial is still beneficial. The logic being that if an attack is inevitable, defense at the very least, minimizes the negative consequence of the attack.

Conclusion

Using Davis's cognitive model, I have argued that deterrence by denial is the most effective deterrence approach for preventing a limited nuclear EMP attack against the United States for three main reasons. First, deterrence by punishment relies heavily on many assumptions such as the validity of the rational actor model, speculating on what potential adversaries value, their perceptions, risk tolerance, decision style and emotional state.[26] These pesky deterrence by punishment issues can be eliminated in this special case by focusing on deterrence by denial in the form of pure defense, which doesn't rely as heavily on understanding the complete psychology of the enemy. Increased resiliency for the civilian power grid is strictly technical in nature and it should be easier to credibly signal our vulnerabilities in this area have been reduced or eliminated and preclude potential adversaries from seriously considering this option. Second, deterrence by denial is proactive versus reactive. In our special case, a good to excellent defense precludes the limited nuclear EMP attack and avoids the necessity to risk escalation in a retaliatory action. Finally, deterrence by denial in this particular case is the more robust option. It provides a complement to deterrence by punishment when the two approaches are be applied simultaneously. Additionally, the defense and deterrence by denial approach has additional benefits above and beyond deterrence, such as protection against natural disasters including solar flares or other weather events. Deterrence by denial in this narrow scope of preventing a limited nuclear EMP attack on the United States is clearly preferable. Putting up a strong and obvious defense through increased resiliency in the civilian infrastructure not only protects our population from being left in the dark, but it also sends a clear and unambiguous message to potential peer aggressors that they will accrue no benefits from their efforts.

To fully implement a deterrence by denial effort, decisive government leadership in a public-private partnership is needed to foster improved transparency, set and enforce federal resiliency standards, and signal to any potential adversaries that our civilian infrastructure has been updated to withstand the perilous threat of an EMP attack. Some might argue that private enterprise always does a better job and that government involvement only means overly bureaucratic standards and regulations, higher costs, and often solutions that are worse than the problems they were intended to correct. In certain areas, I tend to agree, but in areas extremely technical in nature, where the consequences of failure are beyond disastrous, and where there is little monetary incentive for action, the

United States government may be the only entity that can effectively get the job done. This is definitely one of those areas.

First, the effects of a nuclear EMP and the protective measures needed in the civilian infrastructure are extremely technical in nature. Additionally, although many of the particular details on the potential consequences of these effects are classified, we know they can be devastating. Finally, due to the distributed, private, and competitive nature of the American electrical enterprise, there is little financial incentive to invest in resilience improvements against this low probability threat. These three circumstances combined preclude private enterprise from leading this effort and reinforces the need for government leadership in a public-private partnership to meet the EMP attack threat.

Government leadership needs to start with the designation of a single leader, a leader to focus and bring order to the current fragmented, incomplete, and under resourced efforts. In a 2017 *Report to Congress*, some of our nation's top experts in this area concurred stating, "The single most important action that requires immediate action to advance the U.S. Security and Survivability is that the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat." Only through the designation of an executive agent will this effort have any hope of moving past admiring the problem and get down to the tough business of protecting our civilian infrastructure from the threats of an EMP.

More government transparency is another key area needing improvement. Currently, much of what is known about the potential EMP effects to our national infrastructure is extrapolated from classified computer models and thus is difficult to share with industry. This difficulty can and must be overcome because the foundation for preparedness against this EMP threat has to be transparent sharing of relevant information between the government and private utilities. This has been the focus of a 2016 joint effort between the Department of Energy and the Electric Power Research Institute to establish a common public-private EMP resilience strategy. This effort seeks to establish a common framework with consistent goals and objectives to guide government and industry activities.

Along these lines, the establishment of federal infrastructure resilience standards should be a top priority. Established and codified standards will not only guide industry investment, but also support a deterrence by denial strategy against any potential adversaries. The thought here is that if potential adversaries know the infrastructure is resilient, then they will probably decide against this type of attack. Just as important, federal standards will mandate investments in resilience that may not happen otherwise because of the competitive nature of this business sector. The good news here is that experts conclude that "protecting and defending the national electric grid and other critical infrastructure from an EMP attack could be accomplished at reasonable cost and minimal disruption."

There is no doubt that Americans have become accustomed to their technology-enhanced lifestyle. In fact, our society has become so dependent on technology that in its absence we run the real risk of a doomsday struggle for survival. Faced with potential adversaries who might try to leverage this vulnerability, we must move beyond admiring the problem and designate a leader,

an executive agent, who has the authority and the accountability to take concrete actions to mitigate these vulnerabilities. The executive agent needs to be someone who can foster improved transparency and set and enforce federal standards that result in an updated civilian infrastructure to withstand the perilous threat of an EMP attack.

Chapter 4 Notes

1. *2008 Report of the Commission to Assess the Threat to the United States from EMP Attack*. Congress has had committee and subcommittee hearings in 1997 and 1999. Congress subsequently established the commission that issued reports in 2004, 2008, and 2017 that clearly identified vulnerabilities and gave recommendations, but little progress has been made in implementing needed solutions.

2. William R. Forstchen, *One Second After* (New York, N.Y.: Forge Books, 2009).

3. Headquarters, U.S. Air Force/A10 Memorandum for Air University Commander, Subject: AY19 Deterrence Research Topics, Aug 22, 2018

4. Jeffrey W. Knopf, "The Fourth Wave in Deterrence Research," *Contemporary Security Policy*, vol. 31, no. 1 (2010), doi:10.1080/13523261003640819; Wes A. Mitchell, "The Case for Deterrence by Denial," *The American Interest*, Aug. 3, 2017, accessed at www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial; John K. Warden, "Limited Nuclear War: The 21st Century Challenge for the United States," *Livermore Papers on Global Security*, no. 4, (July 2018); Alex S. Wilner, "Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism," *The Journal of Strategic Studies*, vol. 34, no. 1 (2011), pps. 3-37, accessed at https://doi.org/10.1080/01402390.2011.541760.

5. Michael Quinlan, "Deterrence and Deterrability," *Contemporary Security Policy*, vol. 25, no 1 (April 2004), p. 11.

6. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, Mass.: Harvard University Press 1960), p. 9. An oft-cited definition presenting deterrence as "persuading a potential enemy that he should in his own interest avoid certain courses of activity."

7. Wilner, "Deterring the Undeterrable," p. 5.

8. Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press, 1966), p. 23.

9. Henry Sokolski, "Getting MAD: Nuclear Mutual Assured Destruction, Its Origins and Practice," November 2004, accessed Jan. 20, 2019 at http://strategicstudiesinstitute.army.mil/pdffiles/PUB585.pdf.

10. Mitchell, "The Case for Deterrence by Denial,"

11. Warden, "Limited Nuclear War."

12. Ibid.

13. Dennis Bodson, "Electromagnetic Pulse and the Radio Amateur," *QST* magazine, September 1986, pps. 22-26, accessed at www.arrl.org/tis/info/pdf/88615.pdf.

14. George Jacobs, *The NEW Shortwave Propagation Handbook* (Hicksville, N.Y.: CQ Communications, Inc., 1995).

15. "Assessing the Threat from Electromagnetic Pulse (EMP), Volume 1, *Executive Report*, Defense Technical Information Center, accessed at www.dtic.mil/docs/citations/AD1051492.

16. P.R. Barnes, *Effects of Electromagnetic Pulse (EMP) on State and Local Radio Communications Final Report*, October 1973, Oak Ridge National Laboratory; Bodson, "Electromagnetic Pulse and the Radio Amateur;" Michael Kindt, *Building Population Resilience to Terror Attacks: Unlearned Lessons from Military and Civilian Experience* (Maxwell AFB, Ala.: Air University, 2007). These articles describe a variety of commercially available EMP transient-protection devices such as coaxial line suppressors, miniature gas-tube surge protectors, and metal oxide varistors that can be used in grounding, bonding, and shielding applications.

17. Debra K. Rose, "Only in the Mind of the Enemy: Can Deterrence Effectiveness be Measured?," accessed Feb. 27, 2019, at www.researchgate.net/publication/235067689_Only_in_the_Mind_of_the_Enemy_Can_Deterrence_Effectiveness_be_Measured. Author indicates no direct measurement of deterrence is possible and proposes using intelligence indicators to provide feedback for indirectly measuring effectiveness.

18. P. Davis, *Toward Theory for Dissuasion (or Deterrence) by Denial: Using Simple Cognitive Models of Adversary to Inform Strategy*, (Santa Monica, Calif.: RAND Corporation, 2018), accessed at www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1027/RANDWR1027.pdf.

19. This approach is similar to Thomas Mahnken's chapter in *On Limited Nuclear War*, and is intended to help the reader step through the logic of the pros/cons of challenge by punishment or denial.

20. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing, China: PLA Literature and Arts Publishing House, February 1999), pps. 145-146. Authors advocate going beyond traditional boundaries of warfare using unrestricted strikes on a superior adversary's critical nodes to include civilian infrastructure that will cause social panic, street riots, and internal political crisis.

21. Office of the Secretary of Defense, *Nuclear Posture Review* (Washington, D.C.: Department of Defense, Feb. 21, 2018), accessed Jan. 22, 2019, at https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

22. Stephen J. Cimbala, *The Past and Future of Nuclear Deterrence* (Westport, Conn.: Praeger Publishers, 1998).

23. *Fact Sheet: Increasing Transparency in the U.S. Nuclear Weapons Stockpile*, (Washington, D.C.: U.S. Department of Defense, May 3, 2010), accessed Jan. 22, 2019, at https://fas.org/sgp/othergov/dod/stockpile.pdf.

24. "Assessing the Threat from Electromagnetic Pulse (EMP). Volume 1: Executive Report," Defense Technical Information Center, www.dtic.mil/docs/citations/AD1051492.

25. Wilner, "Deterring the Undeterrable," pps. 3-37.

26. Arguably, the United States does not understand some current adversaries, such as North Korea and Iran, as well as it understood the Soviet Union. This makes it harder to know what to "hold at risk" in order to deter those adversaries.

CHAPTER 5

Russian Information Warfare: Precursor to Aggression

Lieutenant Commander Shawn R. Hughes, U.S. Navy

> *"The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures – applied in coordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces. The open use of forces – often under the guise of peacekeeping and crisis regulation – is resorted to only at a certain stage, primarily for the achievement of final success in the conflict."*
>
> – General of the Army Valery Gerasimov
> Chief of the General Staff
> Russian Federation Armed Forces, 2016

In recent years, there has been significant concern about Russia's active engagement in information warfare on its periphery, including Ukraine, Georgia, and the Baltic States of Estonia, Latvia, and Lithuania through both subtle and overt operations designed to reduce North Atlantic Treaty Organization (NATO) influence along its western border. Russia's annexation of Crimea, and the ongoing conflict in Eastern Ukraine are typically cited as proof of Russia's intent and capability. This paper seeks to draw inferences from not only these and other instances, but also from Russian doctrine in an attempt to determine the potential for information warfare to presage increased hostilities in NATO-influenced states. The common consensus is that Russia is not likely to attempt a land grab in the Baltics as it did in Crimea and Eastern Ukraine. However, this does not preclude attempts to foment discord and pressurize the region to reduce NATO influence. As military analysts consider indications and warning signs of potential Russian aggression, emergent Russian information operations should be considered one of the first indicators. This paper explores information operations as precursors to larger Russian aggression campaigns. Several case studies are examined, along

with Russian doctrinal writings to determine the type and timeline of information operations used, as well as the goals information operations are intended to achieve. In some cases, the types of information operations are explicit. However, others must be inferred from the context of operational results. After the information operations are identified and assessed, correlations are drawn between these past actions and potential future Russian military aims. However, there are no set criteria for assessing the degree of threat particular information operations pose, relative to each other or to future aggressive actions. In other words, Russia's conduct of one particular type of information operation versus another may not necessarily provide certain proof that follow-on military action will occur. This paper only speculates about the potential of information operations to lead to future military actions. The types of information operations identified in this paper will help analysts to characterize future Russian actions by providing a limited list of information warfare indicators upon which to focus when conducting indications and warning assessments. Early identification of Russian information operations will allow planners time to devise and implement methods of countering the effects, thereby decreasing the chances of follow-on Russian conventional military actions.

Background

Over the course of the past couple of decades, Russia has employed information warfare techniques as part of an ongoing widespread campaign to influence regional politics and pressure its adversaries to stave off NATO encroachment into states along its border. This behavior is particularly evident during periods of increased tensions, especially when Russia has demonstrated clearly aggressive actions. Several key instances provide appropriate context for identifying and analyzing Russia's use of information operations as an integral part of aggressive action. Russia's 2014 invasion of Ukraine and annexing of Crimea are among the most recent examples of aggression that included information warfare as part of operations. Russia was able to conduct a successful mass media influencing campaign, prior to, during, and after conflict.[1] The 2008 Russo-Georgian War and military action in South Ossetia is another recent example of Russian aggression into a border state in which information operations played a key role. Russia demonstrated classic conventional warfare, mixed with integrated cyberattacks and information warfare to achieve operational as well as strategic effects.[2] The 2007 cyber assault on the Estonian parliament, ministries, banks, and media outlets, largely attributed to Russian sponsored actors, resulted in NATO creating the 'Cooperative Cyber Defence Centre of Excellence' in Tallinn, Estonia. Although this incident did not precede direct military action, many considered it an act of cyberwar on par with conventional military action due to the scope involved. The information warfare incidents above provide sufficient proof that Russia's 2014 and 2016 military doctrines, which discuss its perception of NATO aggression that blends traditional means with nonmilitary capabilities to achieve its objectives, is in full force. The doctrine identifies this hybrid activity as a key threat to Russian security. Media manipulation, propaganda, disinformation, and other information operations are examples of information-related capabilities that are leveraged to

destabilize a government or population in support of larger aggressive actions. Russia has been using these techniques to influence and bolster pro-Russian actors in border states, especially the Baltic States.[3]

Research Question

> *Are there information warfare-related indicators of Russian military aggression designed to deter or limit NATO's influence in the Baltic States?*

Hypotheses

1. *There are information operations that are precursors to Russian aggression.*

2. *Russian information operations are designed to deter NATO influence.*

Literature Review

Several authors provide context for this research. Since this research focuses on indicators and warning signs associated with information warfare leading to further aggression, there are concerns about if, how, and why the United States should deter other nations from conducting information operations aimed at the United States and its allies. As such, only basic deterrence-related concepts are addressed in this context. Lawrence Freedman, in his 2004 book *Deterrence*, provides the necessary definitions and implications of deterrence. He primarily addresses deterrence theory evolution through the advent of nuclear weapons. However, he also applies the concepts of deterrence through denial and punishment in a broader scope that can also be relevant to discussion of information warfare and conventional deterrence.[4] Since the larger context of this research surrounds how NATO might be affected by Russian information warfare, key concepts from Thomas Schelling, in his book *Arms and Influence*, help frame how Russia and NATO view risks, comparative capabilities, and battlespace dynamics. He maintains that, in the event of a resort to nuclear weapons, we should also plan for a war of nerve, demonstration, and of bargaining.[5] This type of planning can also be applied to an information war just as easily. In this case, the weapons need not be nuclear to necessitate additional engagement as part of a conflict. In order to understand the challenges of deriving a warning from a given indicator, Robert Jervis, et al, in their 1985 book *Psychology and Deterrence*, provide insight into validation of indicators, and how actors respond to such warnings.[6] Jervis addresses the need for unambiguous warning, which is seldom associated with information operations, as a key element of deterrent or defensive actions. Inciting a fear of miscalculation can lead to decision paralysis, which is a dominant goal of many types of information operations. These theoretical concepts will help in

understanding how critical it is to identify information warfare indicators prior to outbreak of conventional hostilities.

Research Framework

This paper attempts to answer the research question with a two-pronged approach. First, case study analysis focuses on past incidents in an effort to gain qualitative insights into the types of information operations Russia conducts. This initial analysis provides the scope of information warfare options Russia has employed, which starts to highlight the indicators that American analysts and policymakers should pay attention to when gauging Russia's broader intent during a crisis. The intended result is to correlate Russia's past behaviors and actions to potential future crises. Case study analysis also provides an extrapolated timeline for Russia's use of specific information operations. Understanding the timeline for these types of operations is critical to understanding how an operation was executed in relation to military actions. This helps expand our understanding of warning signs that suggest an information operation may be a precursor to conventional military aggression. The flow of an information operation during the course of conventional aggressive action can then be correlated to similar future actions. Identification of potential similarities between Russia's demonstrated actions and future aggression is possible through case study analysis, and some commonalities and themes become evident. It is these common attributes that will become key indicators of potential Russian aggressive intentions.

The second focus of analysis is a qualitative look at recent Russian doctrine and professional papers written by senior Russian military officers. The purpose of this section is to not only define the degree to which information warfare has been integrated into formal Russian doctrine, but to also understand its prevalence within the thoughts of senior officers. While no two operations are exactly the same, understanding this doctrine does provide a loose framework to identify how Russian information operations fit into military planning. Unfortunately, there is no way to quantify the likelihood of particular information operations being included in a given Russian plan, nor is it my intent to provide such statistics. The goal is to articulate how much emphasis Russia has placed on information warfare in recent years, and correlate this emphasis to a general probability of inclusion in future plans. Some hard data within the source documentation provides a sufficient basis for general statistical characterizations, and, where possible, I provide applicable quantitative analysis to support such points. One area of emphasis is the degree to which Russia has increased the relative importance of information warfare in its military operations. A thorough analysis of Russian doctrine over the past decade offers insights into its profusion.

Fusing Russia's demonstrated use of various information warfare techniques, combined with its degree of doctrinal integration, provides a conclusive understanding of the indicators and warning signs Russia might present before, during, and after its next military aggression campaign. Finding such indications and warnings is the central focus of this research. The goal, however, is not merely to extrapolate a list of past Russian actions. The list must be compiled, of course,

but careful analysis provides the necessary context for correlating Russia's past information operations to potential indicators of future information operations that could lead to follow-on conventional military aggression.

The Information Domain

Understanding what the information domain is requires several definitions up front, especially as I discuss the use of information-related capabilities for military use in achieving political goals. First, *Joint Publication 3-13* defines the information environment as, "The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. [It] is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principal environment of decision making."[7] Information Warfare is the conduct of war within the full scope of the information environment. It is primarily concerned with manipulating information in order to influence the decision-making processes of the adversary leaders or populace. However, certain types of information-related operations, such as cyber and electromagnetic spectrum attacks, can have direct physical effects on the battlefield. *Joint Publication 3-13* defines information operations as, "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[8] Russia also understands the importance of conducting operations within the information environment. Both its 2010 and 2014 military doctrine publications list what Russia considers to be the characteristics of modern warfare conflict. By way of comparison, in 2010, the document places information warfare as the fourth point in a seven-point list, while in 2014, information warfare is integrated into the first three points and even supersedes speed of maneuver and destruction of enemy troops.[9, 10] This research helps contextualize the Russian doctrinal shift to a more information-focused priority in recent years.

Demonstrated Information Operations

Crimea

"An information campaign preceded, accompanied, and followed Russian military operations in Crimea."[11] Michael Kofman, et al, in a 2017 RAND Corporation study, clearly identifies a Russian information campaign within the 2014 military takeover of Crimea. The primary type of information operation identified is the marginalization of domestic independent media outlets, which afforded the Russians greater control and power to shape views in Russia of the events in Ukraine.[12] This spin was partially disinformation, and but mostly involved propaganda to delegitimize the interim government. Kofman asserts that the Russian public was the primary audience of this influence agenda. Also, Kofman suggests a "grass roots" movement was fomented called Stop Maidan, using visual outdoor ads such as tents with logos and banners saying "no to extremism" and "no

to foreign intervention." This campaign was designed to incite the local Crimean populous to rise up against the Maidan government.[13] Kofman also finds, "Moscow leveraged social media effectively to generate domestic support and spread vast amounts of disinformation about the Maidan protests and the intentions of the new government in Kyiv."[14]

Despite clear indications that Russia manipulated the media and engendered dissent among the local population, Kofman, et al, downplays Russian information operations and suggests the efforts were not deliberately tailored information warfare actions integrated into to the Russian offensive into Crimea.[15] Even though, "… the information campaign undoubtedly had a polarizing effect on the population," Kofman maintains that the information-related operations Russia did engage in were simply a byproduct of its domestic messaging campaign that bled over into Crimea. That Russia did not plan its information campaign for Crimea is contrary to most other analysis, but Kofman does provide a necessary counterpoint argument for how Russia incorporated information operations into its annexation of Crimea. Regardless of whether or not Russia specifically planned and implemented information warfare measures for its Crimea incursion, Russia did capitalize on information efforts and inferences can be drawn about the importance of an information warfare campaign in localized conflict. As evidenced by the writings of multiple military officers described in the doctrine review section of this paper, Russia has certainly identified the utility of information warfare and will incorporate its concepts into future plans. Russian actions in Crimea do provide some options that Russia can incorporate into future plans, but they do not provide a validated model for Russian information warfare use.

Eastern Ukraine

According to Kofman et al., multiple information campaigns, and some cyberattacks, were conducted in association with the 2014 Eastern Ukraine separatist conflict.[16] Even before the turmoil intensified in February 2014, the Ukraine government suffered a major distributed denial of service (DDoS) attack. In February, DDoS attacks were conducted against government websites. Kofman claims early attacks were not terribly disruptive, but later attacks compromised the electronic system for compiling election results.[17] Social media was also key in the information campaign.

Kofman states, "Because the two most popular social media platforms in Ukraine, VKontakte and Odnoklassniki, were hosted on Russian servers, Russian authorities were able to block pro-Maidan pages and force service providers to share personal information about those who 'liked' them. Pavel Durov, the founder of VKontakte, sold his remaining stake and fled Russia in April 2014. As violence on the ground escalated, VKontakte and Odnoklassniki provided a tool for soliciting contributions and recruiting in Russia for such groups as 'Anti-Maidan,' 'Donbas People's Militia,' and 'Fund to Help Novorossiya.'"

Social media also captured the activities of the separatists, the Russian equipment being provided to them, and much of the violence waged against them.[19] Russia effectively took over the most common social media platforms and used

them to hinder the Ukrainian government and bolster the separatist movement. This proved to be a most effective method of manipulating the populace's perceptions of events.

Kofman et al, however, conclude that Russia was more successful in influencing Western perceptions than in actually getting results in Ukraine.[20] They find that multiple studies and technical analyses indicate that the impacts of the Russian information campaign were overestimated, and did not elicit the mobilizing effects that were intended. "While the campaign increased hostility toward and distrust of the Ukrainian national government, it did little to mobilize public support of separatism."[21] In the end, Ukraine banned Russian broadcasts as best as it could and the Ukrainian populace actually decreased viewership of Russian news and media outlets. Assessing the effectiveness of Russia's information campaigns in Eastern Ukraine is largely irrelevant to the scope this work. The purpose here is to identify the types of information operations conducted, and whether or not they were precursors to aggression, which in this case fostered a secession movement and led to conventional military action.

Estonia

Lucas Kello summarizes the 2007 cyberattacks in Estonia and explores this new type of "weapon" being brought into strategic operations.[22] He asserts that the use of cyber force is merely a continuance of Soviet/Russian long-standing proclivity for information warfare operations and that influencing the minds of the masses is par for the course. He correlates this to the Russian "reflexive control" doctrine, discussed in the doctrine review section of this paper, and maintains that, for Russia, modern combat centers on domination of the information domain rather than geographic space. Kello's assertions support this paper's goal of tying heavily information warfare-related action to a conventional attack in a future Russian aggression into the Baltics. Kello provides examples of Russian use of information warfare to achieve its goals, and these incidents can be directly correlated to possible future Russian efforts in the Baltic States.[23] Kello identifies the Russian cyberattacks against Estonian vital computer infrastructure as the global starting point for use of cyberoperations to truly affect the economic and governmental affairs of a small nation.[24] Following this incident, much of the world began to consider cybersecurity a vital national interest. However, the information warfare attacks in Estonia did not result in subsequent Russian conventional military operations in the country. As Kello points out, these operations in 2007 are widely regarded as the genesis of this type of cyber external influencing operations. These operations in Estonia may well have been a testing ground for future endeavors. Precipitously, a year later Russia used some of the same techniques ahead of its incursion into South Ossetia in Georgia.

Georgia

Ariel Cohen and Robert E Hamilton, in a June 2011 publication for the Strategic Studies Institute, lay out one of the most comprehensive studies on the

2008 Russian invasion into Georgia.[25] They consider the area of cyberwarfare and information operations to be the "most illuminating area of study," in this conflict.[26] "The war against Georgia marks the first time in its history that Russia has used cyberwar and information operations in support of its conventional operations."[27] This is a powerful indictment, and, as a follow-on to Russian actions in Estonia, seems to be the transition point from testing the application of cyber and information warfare into the realm of full integration with conventional military operations. Cohen and Hamilton assert that Russia attacked 38 Georgian and Western websites at the outset of the war "including those of the Georgian President, the Ministry of Foreign Affairs, the National Bank, the Parliament, the Supreme Court, and the United States and United Kingdom (U.K.) embassies in Georgia."[28] The timing of these attacks is remarkable as well. These attacks were launched nearly simultaneously ahead of the conflict, and stopped within minutes of when Russia announced its ceasefire. The degree of coordination and control is impressive. However, Cohen and Hamilton deem it unlikely that the Russian government conducted the attacks directly. They attribute the attacks to a "shadowy group called the Russian Business Network (RBN), which has not been definitively shown to have links to the Russian government."[29] In fact, Cohen and Hamilton suggest a direct link between the RBN and the cyberattacks in both Estonia the year prior and this case in Georgia. Using a third-party actor affords the Russian military a certain degree of plausible deniability, especially when attribution is difficult to prove.[30]

In this conflict, Russia also engaged in an information campaign to dominate the media narrative in favor of Russian ideals and goals. "The Russian narrative consistently emphasized three major themes. First, Georgia in general and President Mikheil Saakashvili in particular were the aggressors. Second, Russia was forced to intervene in defense of its citizens and to prevent a humanitarian catastrophe. Finally, the United States and the West had no basis on which to criticize Russia because of Western actions in Kosovo and elsewhere."[31] This campaign exhibits many hallmarks of classic information operations, including disinformation, deception, disruption, public influencing, legal/moral justification, and deflection. Russia crafted its narrative to portray itself as the victim and defender, and Georgia played into this scheme, appearing as the offender to most observers.[32] One of the key reasons for Russia's success in its narrative was how closely the government worked with the media. In an unprecedented move, Russia flew approximately 50 reporters to Tskhinvali before the war even started. While not in itself an indication of imminent war, the mass deployment of media personnel is a strong indicator that something important is about to transpire. Overall, Russia was relatively successful in dominating early discourse on the war.[33]

Russian Doctrine Review

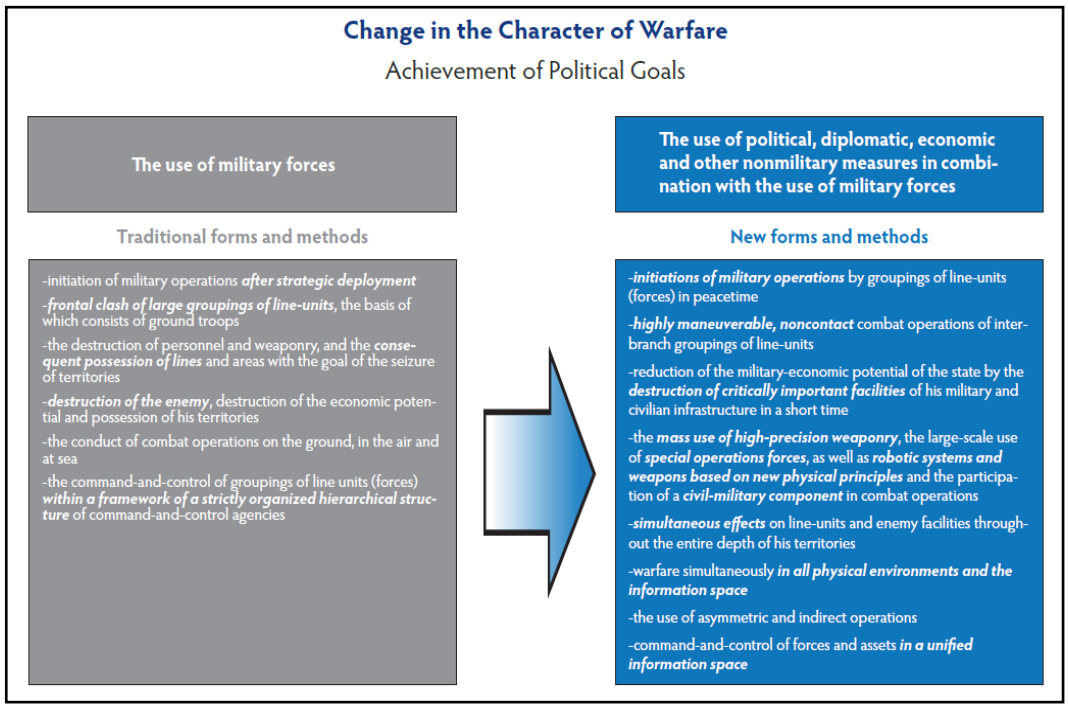
"The intensifying confrontation in the global information arena caused by some countries' aspiration to utilize informational and communication technologies to achieve their geopolitical objectives, including by manipulating public awareness and falsifying history, is exerting an increasing influence on the nature

of the international situation."[34] The 2016 Russian National Security Strategy (RNSS, signed Dec. 31, 2015) essentially accuses "some countries" of conducting information warfare. This passage is largely aimed at the Unites States and its European allies. However, most assuredly, Russia is also one of these countries. The RNSS highlights the information domain 36 times as it articulates the threats, methods of confrontation, and national concerns of Russian leadership. National defense remains the top priority for Russia. Within the context of national defense, Russia states it is developing and implementing informational measures for the purpose of strategic deterrence and the prevention of armed conflicts.[35] However, the measures they are developing can be used offensively as well. The RNSS does not specify the type or scope of information operations Russia has at its disposal. In order to better understand Russia's options, a deeper look into the writings of Russian military leaders is warranted. The best place to start is at the top.

Russian General of the Army Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces, is a prolific author of Russian military policy. According to Gerasimov, "The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures – applied in coordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces. The open use of forces – often under the guise of peacekeeping and crisis regulation – is resorted to only at a certain stage, primarily for the achievement of final success in the conflict."[36]

This description is precisely what this paper is intended to address. As previously described in the case studies above, with the exception of Estonia, each of the Russian military actions was conducted in conjunction with information warfare-related operations occurring before, during, and after crisis regulation or peacekeeping force deployment. The method General Gerasimov describes is not only an accurate description of Russia's recent conquests, but it now appears to be a reflection of Russian military core doctrine. Gerasimov illustrates the transition of Russian forms and methods of warfare in a modern context in an article (in *Figure 1*) and as indicated, special emphasis is now placed on operations in "information space."[37]

Figure 1. Change in Character of Warfare



(Gerasimov article in Voyenno-Promyshlennyy Kurier *Feb. 26, 2013, translated by Charles Bartles)*

Two prominent Russian military officers, Col. S. G. Chekinov and Lt. Gen. S. A. Bogdanov, provide an analysis in 2016 of globalization on military operations.[38] According to Chekinov and Bogdanov, "It is an axiom that the country superior in the forces and information warfare capabilities can count on leadership in the military and political sphere, and can have a military strategic advantage."[39] The inference here is that the combat forces and information forces are considered equal in importance to achieving advantage over an adversary. This is a relatively new concept, from a warfighter perspective. Historically, information-related capabilities have always been relegated to a subservient or supportive role to the combat arms. However, we now see information warfare forces coming to the forefront in recent engagements. Additionally, Chekinov and Bogdanov stress the importance of information capabilities, and the information environment, being integrated into the operations of all military organizations at every level of military operations, from the strategic on down to the tactical.[40] In another 2016 article, Chekinov and Bogdanov state, "A special place in the system of indirect moves will belong to information and special operations and actions. Targeted cyberattacks on a systematic basis will be carried out both by state special services and private persons."[41] This statement could be the preamble to a summary of the information operations conducted in Estonia, Crimea, and Ukraine. Chekinov and Bogdanov clearly subscribe to information warfare as the way ahead when they state, 'In the new conditions of the 21st century and evolution of military art, it is precisely military strategy that is to develop the theory of foundations of national

and state military security with extensively used information support (indirect moves)."[42]

Reflexive control (RC) is another Russian information warfare doctrinal concept that has prompted curiosity in analysts. A 2004 article by Timothy L. Thomas provides a very clear analysis of what this theory entails and how the Russian military has adopted the construct. Thomas defines RC as, " … a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[43] In other words, Russian will construct a scenario and disseminate as much information as possible to its opponent such that the opponent, based on these inputs, will make a decision favorable to Russia. "The Soviet and Russian Armed Forces have long studied the use of reflexive control theory, particularly at the tactical and operational levels, both for maskirovka (deception) and disinformation purposes and, potentially, to control the enemy's decision-making processes."[44] Thomas asserts that this form of information manipulation has been part of the former Soviet and Russian toolkit for most of the 1990s and notes that Major General N. I. Turko, an instructor at the Russian Federation's General Staff Academy, views RC as, " … an information weapon that is more important in achieving military objectives than traditional firepower."[45] The types of information operations associated with RC include: camouflage (at all levels), disinformation, encouragement, blackmail by force, and the compromising of various officials and officers.[46] According to Thomas, the most concerning application of Russian RC is its employment to affect a state's decision-making process by use of carefully tailored information, and "the most significant of those threatening actions is disinformation that seeks to exert a goal-oriented effect on public opinion or on decision-makers."[47]

When comparing Russia's 2010 and 2014 official documents of military doctrine, it is interesting, but hardly surprising, that the 2010 document contains no mention of "information and communication technologies in the military-political purposes," while by 2014, this area becomes one of the primary external military dangers to Russia.[48, 49] Another notable distinction between these two documents is the content below from the first four, and presumably prioritized, items in the "Characteristics" of modern warfare sections within each document.[50, 51]

2010 Russian Military Doctrine

1. The integrated utilization of military force and forces and resources of a nonmilitary character.

2. The massive utilization of weapons and military equipment systems based on new physical principles that are comparable to nuclear weapons in terms of effectiveness.

3. The broadening of the scale of the utilization of troops (forces) and resources operating in airspace and outer space.

4. The intensification of the role of information warfare.

2014 Russian Military Doctrine

1. Integrated use of military force, political, economic, informational, and other nonmilitary measures nature, implemented with the extensive use of the protest potential of the population, and special operations forces.

2. Massive use of weapons systems and military technology, precision, hypersonic weapons, their means electronic warfare, weapons based on new physical principles, comparable in efficiency with nuclear weapons, management information systems, and unmanned aircraft and autonomous marine vehicles, controlled robotic weapons and military equipment.

3. The effect on the enemy throughout the depth of its territory simultaneously in the global information space, aerospace, land, and sea.

4. Selectivity and a high degree of destruction of objects, speed maneuver troops (forces) and the fire, the use of various mobile groups of troops (forces).

Notice how the lower ranked and generic "4. The intensification of the role of information warfare," in 2010, expands into and permeates the first three characteristics in the 2014 doctrine, even ahead of the use of combat forces. This is quite a remarkable shift, and highlights a drastic change in Russian perceptions of the importance of the information domain and information warfare in military operations.

The recent evolution of Russian doctrine toward increased emphasis on information warfare as a core element of military operations does not come as a surprise. The rapid expansion of the information domain over the course of several decades was bound to carry over into the realm of military purview, and, like the United States, Russia has been taking steps to keep up with technology to ensure it retains its place as a global power. Information warfare is a significant component

within Russia's military construct, and the United States must be ever vigilant for indications that Russian information operations are designed to presage conventional military aggression.

Key Findings

According to a 2018 RAND Corporation study, Russia is engaged in a global information operations campaign. "In this confrontation, Russia uses propaganda, cyberoperations, and proxies to influence neighboring and Western countries. A state-funded Russian television network, Russia Today, broadcasts abroad in English, Arabic, and Spanish. State-controlled news websites, such as Sputnik, disseminate news in about 30 languages. Russia also coordinates its covert information activities, such as cyberwarfare and non-attributed social media trolls or bots, with its more public media campaign, as was reported in the 2016 U.S. elections."[52]

The types of information operations observed in the four cases presented were clearly designed to influence, disrupt, corrupt, or usurp the decision-making cycles of the countries involved. In Crimea, the marginalization of local media outlets allowed Russia to press its own propaganda and influence the local population's opinions. The disinformation campaign masked how and why events actually played out, resulting in local views favorable to the Russian agenda. In Eastern Ukraine, DDoS attacks and a heavy-handed social media influencing campaign were clearly precursors to aggression, which in this case fostered a secession movement and led to conflict. DDoS attacks tend to focus on breaking the decision-making cycle of an opponent by limiting information sources and communications methods of leaders. The social media campaign was largely successful in influencing the locals to action through disinformation. Russia also pressed its advantage in news media, until Ukraine shut down most Russian speaking outlets. In Estonia, despite a lack of conventional military action, its cyber and information operations provided Russia with critical data on the effects of such operations. Estonia proved that information warfare is a viable method of conflict on its own. It must be noted that Estonia is a NATO member, and it is quite remarkable that Russia did not engage conventional military forces in Estonia, whereas in non-NATO Crimea, Ukraine, and Georgia, Russia did employ forces. This suggests the NATO umbrella does provide credible deterrence against Russian conventional aggression. In Georgia, Russia merged information warfare with conventional military operations by conducting cyberattacks against Georgian websites to deny or alter information and influencing the population through social media and tight narrative control in the news media while sequentially "protecting" its Russian-speaking constituents by deploying military units into Georgia.

Table 1 below reflects the information warfare-related operations demonstrated in these four cases in a comprehensive format relative to timing of military force employment.

Table 1: Information Operations across Time

Type	Before Conflict	During Conflict	After Conflict
Cyberattack (Denial of Service)	C, U, E, G	C, U, G	
Cyberattack (Disruption)	C, U, E, G	C, U, G	
News Media Influence (Disinformation) (Information Masking)	C, U, E, G	C, U, G	C, U, G
Blackmail (Leader Influence) (Corruption)		U	
Decision-cycle Influence (Disinformation) (Deception)	C, U, E, G	C, U, G	C, U, G
Social Media Influence (Disinformation) (Deception)	C, U, E, G	C, U, G	C, U, G

(C-Crimea, U-Eastern Ukraine, E-Estonia, G-Georgia)

Russian military doctrine has morphed over the past decade as information warfare has risen to the forefront of military operations world-wide. Russia's top priority is its national defense. The information operations it has developed and implemented are geared toward strategic deterrence. Russia claims its efforts are for the prevention of armed conflicts. However, this research shows that Russia employs information warfare offensively, in many cases with the intent to foment and justify armed conflicts. Top Russian military officers, such as General Gerasimov, tout the information domain as the most important warfighting arena in the modern world. Information operations are now an integral part of larger Russian military endeavors, and in most cases are conducted before, during and after conventional armed conflict. Reflexive Control, the decade-old Russian theory of manipulating target audiences with carefully orchestrated information feeds, appears to be the basis of much of Russia's recent news and social media influencing campaigns. These efforts allowed Russia to steer populations' perceptions of events, and not just in finite geographical areas, such that local conditions favor the Russian narrative. It is not a surprise that Russia has embraced the information age, both politically and militarily. Russia has growing resources, and the availability to free-agent information warriors adds an element of non-

attribution that allows the Russian military to explore military options in the information domain with plausible deniability. As this research demonstrates, the most concerning aspect of Russia's new military reliance on information warfare is a scenario in which a focused information campaign is followed by a conventional force incursion as General Gerasimov articulates.

Conclusion

The implications of this research are important for American military planners. Understanding how and when Russia will utilize its extensive information warfare capabilities will be key to identifying and countering future Russian aggression. The Baltic States, due to Russian perceptions of influence, are likely to bear the brunt of future information warfare aggression. If a Russian information campaign is identified, the challenge will be to determine if it is a precursor to a larger hostile initiative. The information operations identified herein should validate indications and warning criteria already established and as future indicators become available through the various collection means, warning signs of impending aggression may follow. While there does not currently appear to be any glaring signs of conventional Russian military aggression toward the Baltic States, such goals cannot be discounted simply due to lack of indicators. Although Russian intent, as with most nations, is always difficult to discern when it comes to use of asymmetric capabilities in the information environment, it is clear that Russia will continue to exert influence over regional and even global events to establish favorable conditions for its resurgent aspirations. Since the collapse of the former Soviet Union, Russia has sought to limit NATO's influence and expansion along its borders. Based on this research, NATO is clearly not a deterrent against Russian information warfare against a Baltic state. There is, however, some evidence to suggest Russia will not follow an information campaign with conventional force in a NATO-aligned country, as demonstrated in Estonia. Are Russian actions in non-NATO countries designed to demonstrate resolve and thus deter these countries from engaging with NATO? Are Russian information operations conducted in NATO-aligned countries designed to deter further NATO expansion? The answer to both of these questions seems to be yes. While NATO continues to provide a deterrent against conventional military actions in a NATO-aligned state, there may be a tipping point in the future in which Russia perceives NATO influence has gone too far. When this occurs, Russian information operations will then precede a conventional military conflict resembling, in many ways, the cases noted here. More research is needed to understand how Russia can be deterred from engaging in information warfare and thus limit Russia's ability to conduct hostile information operations against U.S. interests. However, if the United States and NATO fail to deter Russia from engaging in information warfare, early identification of Russian information operations will help maximize decision space for implementing countermeasures, which is becoming increasingly vital in the high-speed modern age.

Chapter 5 Notes

1. Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, Calif.: RAND Corporation, 2017), pps. 70-83

2. Col. George T. Donovan, Jr., *Russian Operational Art in the Russo-Georgian War of 2008*, (Carlisle Barracks, Pa.: U.S. Army War College, 2009), p. 9

3. Bryan Frederick, Matthew Povlock, Stephen Watts, Miranda Priebe, Edward Geist, *Assessing Russian Reactions to U.S. and NATO Posture Enhancements* (Santa Monica, Calif.: RAND Corporation, 2017), p. 30

4. Lawrence Freedman, *Deterrence* (Malden, Mass.: Polity Press, 2004), pps. 36-40

5. Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press, 2008), p. 111-114

6. Robert Jervis, Richard Ned Lebow, and Janice Gross Stein, *Psychology and Deterrence* (Baltimore, Md.: Johns Hopkins University Press, 1991), pps. 75-76

7. *Department of Defense Joint Publication 3-13* (Washington, D.C.: U.S. Department of Defense, 2006), p. I-1

8. Ibid.

9. Vladimir Putin, "The Military Doctrine of the Russian Federation." approved by Russian Federation presidential edict 2010, p. 5.

10. Vladimir Putin, "The Military Doctrine of the Russian Federation." approved by Russian Federation presidential edict 2014, p. 4.

11. Kofman, et al, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, p. 12.

12. Ibid.

13. Ibid., p. 15.

14. Ibid., p. 28.

15. Ibid., pps. 1-77.

16. Ibid., pps. 50-60.

17. Ibid., p. 50.

18. Ibid.

19. Ibid., p. 50.

20. Ibid., p. 54.

21. Ibid.

22. Lucas Kello, *The Virtual Weapon and International Order* (New Haven, Conn.: Yale University Press. 2017), pps. 212-228.

23. Ibid.

24. Ibid., p. 212.

25. Ariel Cohen and Robert E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications* (Carlisle Barracks, Pa.: U.S. Army War College Strategic Studies Institute, June 2011), pps. 1-100.

26. Ibid., p. 44.

27. Ibid.

28. Ibid.

29. Ibid., p. 45.

30. Ibid.

31. Ibid., p. 46.

32. Ibid., p. 47.

33. Ibid., p. 48.

34. Russian Federation, "Russian National Security Strategy, December 2015 – Full-text Translation", (Moscow, Russia: The Kremlin, Dec. 31, 2015), p. 5.

35. Ibid., p. 7.

36. Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military-Industrial Kurier*, Feb. 27, 2013, translated from Russian on June 21, 2014, by Robert Coalson, editor, *Central News*, Radio Free Europe/Radio Liberty (2014), p. 1-8 (originally 23-29).

37. Gerasimov, "The Value of Science Is in the Foresight," p. 25.

38. S. G. Chekinov, S. A. Bogdanov, "The Distinctive Features of Military Security Provision in 21st Century Russia in Conditions of Globalization," *Military Thought*, vol. 0025, no. 2, (2016), pps. 1-16.

39. Ibid., p. 6.

40. Ibid.

41. S. G. Chekinov, S. A. Bogdanov, "Military Strategy: Looking Ahead." *Military Thought*, vol. 0025, no. 4, (2016), p. 34.

42. Ibid., p. 35.

43. Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies 17* (2004), p. 237.

44. Ibid., p. 239.

45. Ibid., p. 240.

46. Ibid., p. 242.

47. Ibid., p. 254.

48. Putin, “The Military Doctrine of the Russian Federation.” 2010, p. 5.

49. Putin, “The Military Doctrine of the Russian Federation.” 2014, p. 4.

50. Putin, “The Military Doctrine of the Russian Federation.” 2010, p. 5.

51. Putin, “The Military Doctrine of the Russian Federation.” 2014, p. 4.

52. Todd C. Helmas, et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, Calif.: RAND Corporation, 2018), p. 1.

CHAPTER 6

Conclusion

The papers in this manuscript have thoughtfully explored how adversarial conceptions of deterrence may differ from U.S. conceptions and what this means for the United States government moving forward with planning and strategy. Taken together, they yield several conclusions and policy recommendations.

Firstly, each of the four papers in this manuscript highlighted the need for more serious discussion of how the United States will handle strategies of escalation or entanglement if used by adversarial states such as Russia in response to various scenarios across the spectrum of conflict. Further, and importantly, the papers in this manuscript have shown the very real and practical need to understand how different actors view the importance of deterrence. For instance, better understanding the rivalry between India and Pakistan gives us a better understanding of how nuclear powers manage escalation and crisis scenarios, broadening the scope out from Russia and the United States during the Cold War. Finally, the papers in this manuscript highlight the importance of readying the homeland for high-altitude electromagnetic pulse (HEMP) attacks from a range of potential adversaries, from a nonstate actor to a peer competitor.

With this in mind, policy recommendations center around the need for a more cohesive understanding of deterrence and the role that nuclear weapons play in both a U.S. context as well as adversarial countries such as Russia. The 2018 *Nuclear Posture Review* calls out a return to great power competition, indicating that the nuclear threat faced by the United States is more dynamic than ever before. The role that new technology plays in Russian and Chinese strategies of deterrence is important and understanding how nuclear weapons fit within each country's spectrum of conflict will help ensure the United States is able to adapt. Further, as nuclear proliferation continues to be a concern to the United States, particularly in light of recent events in regard to Iran and how neighboring countries such as Saudi Arabia may respond, it is shortsighted for American scholars and practitioners to assume that new proliferators will behave as previous proliferators have. The papers in this series have shown how the United States can better prepare the homeland through a better understanding of adversarial nuclear capabilities and strategies.

USAF Center for Strategic Deterrence Studies
Maxwell Air Force Base, Alabama

Providing Research and Education on
WMD Threats and Response for the US Air Force