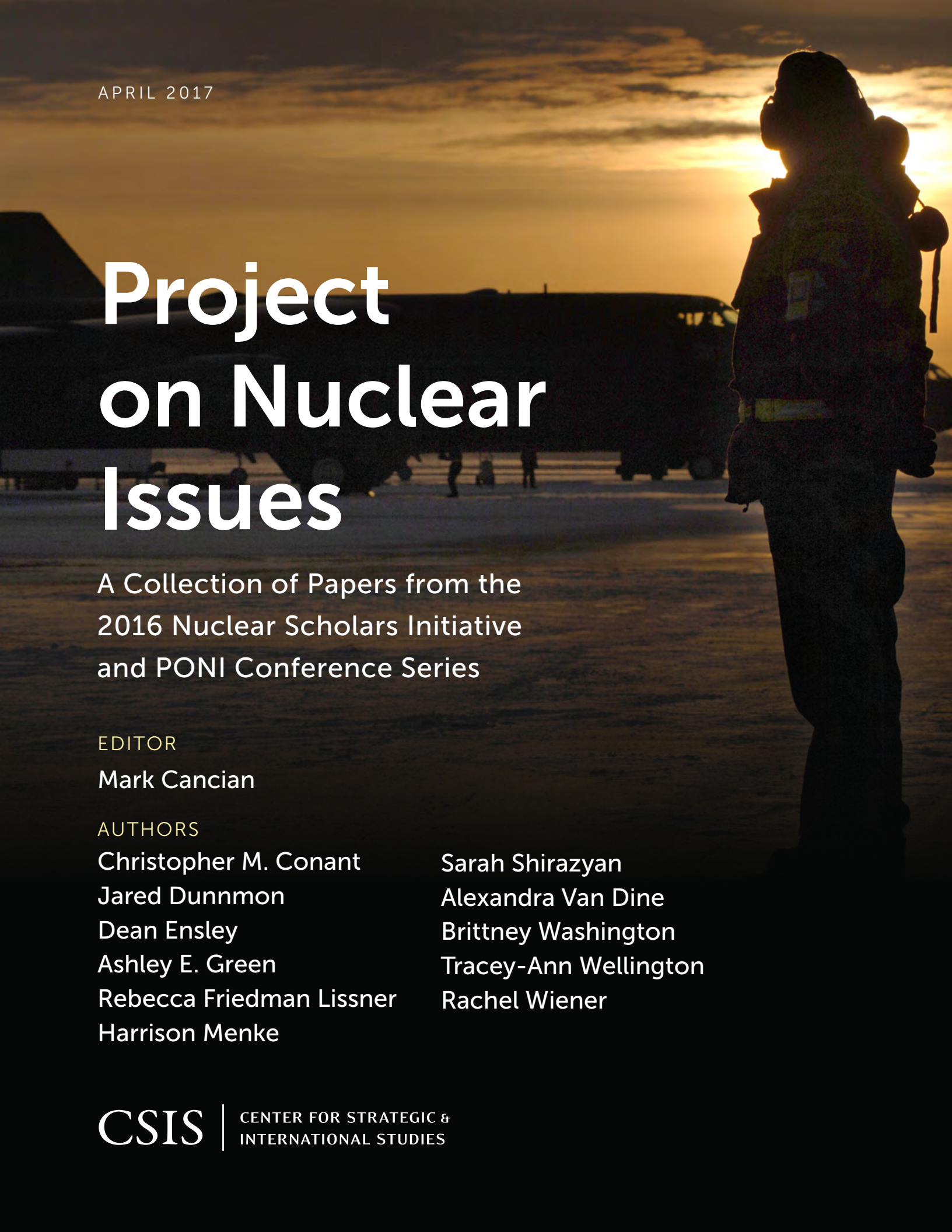


APRIL 2017

Project on Nuclear Issues

A Collection of Papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series

EDITOR

Mark Cancian

AUTHORS

Christopher M. Conant
Jared Dunnmon
Dean Ensley
Ashley E. Green
Rebecca Friedman Lissner
Harrison Menke
Sarah Shirazyan
Alexandra Van Dine
Brittney Washington
Tracey-Ann Wellington
Rachel Wiener

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

APRIL 2017

Project on Nuclear Issues

A Collection of Papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series

EDITOR

Mark Cancian

AUTHORS

Christopher M. Conant
Jared Dunnmon
Dean Ensley
Ashley E. Green
Rebecca Friedman Lissner
Harrison Menke
Sarah Shirazyan
Alexandra Van Dine
Brittney Washington
Tracey-Ann Wellington
Rachel Wiener

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

This report is made possible by the generous support of the Defense Threat Reduction Agency and the National Nuclear Security Administration.

ISBN: 978-1-4422-8001-4 (pb); 978-1-4422-8002-1 (eBook)

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.**csis**.org

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.**rowman**.com

Contents

Introduction

Sarah Minot[1]

The role that nuclear weapons play in international security has changed since the end of the Cold War, but the need to maintain and replenish the human infrastructure for supporting nuclear capabilities and dealing with the multitude of nuclear challenges remains essential. Recognizing this challenge, CSIS launched the Project on Nuclear Issues (PONI) in 2003 to develop the next generation of policy, technical, and operational nuclear professionals through outreach, mentorship, research and debate. PONI runs two signature programs—the Nuclear Scholars Initiative and the Annual Conference Series—to engage emerging nuclear experts in thoughtful and informed debate and research over how to best address the nuclear community's most pressing problems. The papers included in this volume comprise research from participants in the 2016 Nuclear Scholars Initiative and the PONI Conference Series. PONI sponsors this research to provide a forum for facilitating new and innovative thinking and to provide a platform for emerging thought leaders across the nuclear enterprise. Spanning a wide range of technical and policy issues, these selected papers further discussion in their respective areas.

PONI owes many thanks to the authors for their dedication and outstanding work. Particular appreciation goes to the senior experts who provided mentorship for the research papers, those who came to speak to the Nuclear Scholars during their workshop sessions, and those who moderated conference panels. PONI could not function without the generosity of these knowledgeable individuals.

Lastly, PONI would like to express its gratitude to our partners for their continued support, especially the Defense Threat Reduction Agency and the National Nuclear Security Administration.

---

1. Sarah Minot is the program manager and research associate with the Project on Nuclear Issues at CSIS. She holds an MA in conflict resolution from Georgetown University and a BA in political science and international relations from the College of Wooster.

Building Next Generation Global Strike Bomber Readiness and Personnel

Christopher M. Conant[1]

The global security landscape has become increasingly multifaceted, dynamic, and unpredictable across the spectrum of conflict. This is easily apparent in what many consider a foundation of the United States' security posture: rapid global strike. Following the end of the Cold War, national security scholars and practitioners prioritized conventional warfare within global strike, allowing the equally significant role of nuclear warfare to atrophy. Emerging twenty-first century security realisms will not afford the United States the luxury of ignoring issues and challenges present in constructing and executing full-spectrum global power missions. A re-analysis of operational readiness and human capital methodologies, viewed through a dual-doctrine[2] lens, is required to ensure a global strike force prepared for next generation combat and deterrence.

INTRODUCTION

Global strike operations consist of a harmony between weapons systems, people who operate those systems, and the doctrine guiding employment. These variables must undergo a thoughtful reinvigoration to be ready for the twenty-first century security landscape. The Department of Defense (DoD) has historically succeeded in maintaining a technological edge over current and future adversaries. However, this assumption is at risk, as implied by the current commander of United States Strategic Command (USSTRATCOM) whom stated, "to be clear . . . baseline

1. Christopher M. Conant is a major in the U.S. Air Force. He has flown both the B-52H Stratofortress and the B-2A Sprit bombers. The views expressed in this research paper are those of the author only and do not reflect the official policy or position of the U.S. government or the Department of Defense.

2. Dual doctrine refers to both conventional and nuclear operational capability.

sustainment won't meet future adversarial threats."[3] Moreover, equally important advancements in global strike doctrine and people are at risk of lagging behind.

Global strike doctrine and strategic deterrence theory result from both a *capability* and a *will* to use that capability. Strategic deterrence is reliant on a cohesive relationship between all national elements of power: diplomatic, information, military, and economic (DIME). While those components do not exist in a vacuum, for Global Strike Command, the primary element of DIME is military deterrence. Twenty-first century conventional and nuclear power must possess the proper integration of priority to create a holistic and effective posture. Most critical to that process is combat *capability*. An entity could possess the unlimited *will* to act; however, if that will is not supported by *capability*, then the overall deterrence effect is absent. Conversely, an entity can possess validated *capability*, and despite the stated *will* to use that capability, they are taken seriously. Without capability there cannot be a credible *will*.

There are more nuclear-armed countries now than during the Cold War. Today, the number of nuclear-armed states is at risk of increasing. Due to this reality, according to the editors of *Strategy in the Second Nuclear Age*, "nuclear rollback is a remote prospect at best," meaning the role of nuclear weapons could increase over the coming decades.[4] Simultaneously, the championing of strategic airpower and its vast effects on the international security landscape has decreased due to fifteen consecutive years of land-based conflicts within a permissive air and space environment. The often-forgotten fact is that strategic airpower forces (e.g., bombers, tankers, reconnaissance, ballistic missiles) over the past 70 years have, at a comparatively low cost, "delivered on the promise of peace that was once dismissed as fanciful dreams."[5] Strategic global strike readiness postures may become *more* important to international stability than at any previous point in history. Yet, among scholars, policymakers, and military strategists, there is no agreement on a twenty-first century strategic deterrence posture.

Recently, the secretary of the Air Force and senior military leadership initiated long overdue upgrades to the United States' global strike industry. The erosion of critical nuclear infrastructure is unacceptable and dangerous. Additionally, the DoD must holistically ensure the number one priority is the development of combat personnel.

The first part of this paper discusses the relationship between deterrence and combat capability by defining the readiness posture required for the twenty-first century. Essential to note are two key points: AFGSC assets have a unique requirement of readiness to maintain, and theories of deterrence are inherently abstract and absent specific metrics. Hence, when a force builds priorities around deterrence, inefficient military readiness can result. This is detrimental to both combat

3. Terri Moon Cronk, "STRATCOM [Strategic Command] Commander Addresses Strategic Deterrence in 21st Century," *DOD News*, October 24, 2016.

4. Toshi Yoshihara and James R. Holmes, "Conclusion: Thinking about Strategy in the Second Nuclear Age," in *Strategy in the Second Nuclear Age: Power, Ambition, and the Ultimate Weapon*, ed. Toshi Yoshihara and James R. Holmes (Washington, DC: Georgetown University Press, 2012), 225.

5. Paul Darling, "Figure Out the Air Force: Airpower, Nuclear Weapons and Next Generation Bombers," *Cicero Magazine*, July 6, 2015, http://ciceromagazine.com/features/figure-out-the-air-force-airpower-nuclear-weapons-and-the-next-generation-bomber/.

power and deterrence effectiveness. As an alternative, focusing first on combat capability allows strategy (and readiness) to become correctly prioritized and inherently measurable, with a ripple effect of amplified deterrence. This paper will present two recommendations to address these issues.

The second portion of the paper explores how AFGSC can institute a vision and plan for innovating and molding airmen into global strike warriors prepared for the next generation fight. The greatest effect on combat capability is from people, not technology. As General George Patton famously stated, "wars may be fought with weapons, but they are won by men [and women]." Seizing on recent shifts in momentum toward systematic change in the management of personnel, a third recommendation is presented showing how AFGSC can prepare and retain global strike operators.

OPERATIONAL READINESS FOR TWENTY-FIRST CENTURY COMBAT

The 2015 National Security Strategy (NSS) outlines a lengthy list of requirements for the DoD. There are eight major priority items, which cover everything from catastrophic attack on the homeland to climate change.[6] Most importantly, the delineation of priorities is blurred, highlighting a recurring theme within many grand strategic documents: the requirement to be a global power, ready for any possible contingency. This strategic landscape where change is the norm, presents a significant challenge to designing and updating strategic, operational and tactical priorities.

The 2014 Quadrennial Defense Review (QDR) outlines the all-encompassing requirements for twenty-first century military assets:

> U.S. Armed Forces will be capable of *simultaneously* defending the homeland . . . and in *multiple regions*, deterring aggression and assuring allies through forward presence and engagement. If deterrence fails *at any given time*, U.S. forces will be capable of defeating a regional adversary in a large-scale multi-phased campaign, *and* denying the objectives of . . . a *second aggressor in another region*.[7]

The U.S. Air Force (USAF) 2015 and 2016 posture statements express requirements for a dual-doctrine strike force as being able to "credibly threaten and effectively hold any target on the planet at risk."[8] The ability to achieve these global strategic demands comes at an extremely high cost in human and resource capital. It is apparent from the national level to the Air Force level, the above strategic documents lack specificity. While it is not strategically incorrect, in theory, to "be

6. White House, *National Security Strategy, February 2015* (Washington, DC: White House, 2015), 8, http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf.

7. Department of Defense (DoD), *Quadrennial Defense Review 2014* (Washington, DC: DoD, 2014), vi, http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf. Emphasis added.

8. Deborah Lees James and General Mark A. Welsh III, "Fiscal Year 2015 Air Force Posture Statement," Department of the Air Force, March 2014, 17.

ready for anything, anytime," it is incongruous to communicate that demand without clear and measurable priorities to achieve such an objective. Additionally, the ability to achieve these global strategic demands come at an extremely high cost in human and resource capital. The necessary resources to accomplish the goal must be provided.

National security strategies rely heavily on strategic deterrence theory. The concept of deterrence is "the use of threats by one party to convince another party to refrain from initiating some course of action."[9] Fundamentally, deterrence is the ability to influence a decisionmaking process, to convince an entity not do something they may otherwise do. Deterrence efficacy is challenging because the targeted entity determines effectiveness. It is impossible to be inside the mind of an adversary; hence, strategists seldom know exactly when, or how, deterrence will work.

Deterrence theory and capability are intimately related, but must be broken apart and prioritized correctly. A credible deterrent results from a capability, not simply an idea. Moreover, for military operators the primary focus is in "capability," not "will," as the will to use force is the responsibility of elected officials. This means military deterrence theory is *only conclusive if a viable combat capability exists*. When military theory prioritizes deterrence in place of, or before, combat capability, dual doctrine operations and military force readiness are ill prepared for twenty-first century combat. This in turn undermines deterrence effectiveness.

The Challenges of Deterrence

The Air Force is aggressively pushing the reinvigoration of deterrence theory within global strike doctrine. However, deterrence theory remains an abstract and fundamentally contested domain between scholars and policymakers. Considered the pioneer of deterrence, Thomas Schelling's ideas, when viewed through a twenty-first century lens, are foundationally timeless, yet arguably have shortcomings in identifying the psychological effect of a target. As a result, a growing recognition of a "huge psychological deficiency in the theory of rational deterrence" is challenging many previous assumptions.[10] Some scholars argue that deterrence operations over the coming decades must take on a new form of thinking, whereby the *what*, not *who*, to deter should be the focus.[11] In many ways, the *what* (i.e., a physical target or system) is easier to measure, as actions and results are immediately seen (the target was destroyed, or the enemy forces retreated).

Two leading airpower theorists, Colonels John Warden and John Boyd, presented ideas applicable to the molding of deterrence methodologies into operational strategy. In Warden's argument for the importance of "getting inside the enemy's head" and "knowing what the enemy

9. P. K. Huth, "Deterrence and International Conflict: Empirical Findings and Theoretical Debate," *Annual Review of Political Science* 2, no. 1 (June 1999): 25–48.

10. James G. Blight, "The New Psychology of War and Peace," review of *Psychology and Deterrence*, by Robert Jervis et al., *International Security* 11, no. 3 (Winter 1986/1987): 182.

11. Joshua Rovner, "After Proliferation: Deterrence Theory and Emerging Nuclear Powers," in Yoshihara and Holmes, *Strategy in the Second Nuclear Age*, 21.

leadership values," there is an emphasis placed on the *who, or* the psychology of combat.[12] Boyd alternatively concentrated on physical targets, or the *what*, when trying to coerce an enemy's behavior.[13]

Regardless of divergent viewpoints between scholars, it is certain that the psychological effect of a capability on an adversary can be immensely tough to quantify. Absent a clear consensus, deterrence theory can fall into the realm of ambiguity. Sometimes this is done deliberately, to complicate an adversary's decision calculus.[14] However, ambiguity may result in one of the following outcomes: operational vagueness, a strategy for every possible situation, or no effective strategy at all.

Military operators live in a reality defined by measurable objectives. Ambiguity complicates military planning. Without establishing a desired effect against a specific objective, operational plans lack efficiency, or a method to judge success or failure. This contrasts with deterrence theory. Ultimately, "the absence of a [nuclear] attack, or a conventional attack by another state, against the U.S. is not, ipso facto, evidence that this overall force structure has actually *deterred* potential wrongdoers" as "successful deterrence is impossible, or almost so, to gauge."[15] Warden ultimately recognized similar challenges within his own strategy, as it was his "personal belief that the psychological factor is excessively difficult to measure," which led him to "direct his effort primarily against the enemy's physical nature."[16] Deterrence, then, "can be a desirable goal but an impossible guide," and often a "concept that requires unavailable data about unknown processes, that is not empirically testable, and that cannot be shown to be working."[17]

Combat Capability versus Deterrence Theory

The Schlesinger Report argued that within the DoD there was "a failure to appreciate the larger role of deterrence—as opposed to warfighting capability."[18] The dichotomy between deterrence and capability is significant, in knowing where airpower should focus effort. Both are important, yet priority between focusing on deterrence vs. capability matters operationally and culturally.

---

12. Alan Stephens, "Fifth Generation Strategy," in *Airpower Reborn*, ed. John Andreas Olsen (Annapolis, MD: Naval Institute Press, 2015), 140–141.

13. Ibid., 142.

14. Kevin Chilton and Greg Weaver, "Waging Deterrence in the Twenty-First Century," *Strategic Studies Quarterly* 3, no. 1 (Spring 2009): 32, http://www.au.af.mil/au/ssq/2009/Spring/chilton.pdf.

15. Jeff Keuter and John B. Sheldon, "Introduction," in *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century*, ed. Robert Butterworth et al. (Washington, DC: George C. Marshall Institute, 2011), 1, http://marshall.org/wp-content/uploads/2013/08/Butterworth-et-al-Returning-to-Fundamentals-Deterrence-and-U.S.-National-Security-in-the-21st-Century-Roundtable.pdf.

16. Stephens, "Fifth Generation Strategy," 140–141.

17. Robert L. Butterworth, "Nuclear Force Planning: Odin or Onan?," in Butterworth et al., *Returning to Fundamentals*, 14.

18. James Schlesinger, *Phase II, Review of the DoD Nuclear Mission*, Report of the Secretary of Defense Task Force on DoD Nuclear Weapons Management (Washington, DC: Department of Defense, 2008), 3.

Military deterrence and combat capability are complementary, but easily blurred in distinction. Global strike practitioners risk focusing on and prioritizing too heavily on the former to the detriment of the latter. Former Chairman of the Joint Chiefs of Staff, General Nathan F. Twining correctly stated, "forces that cannot win, will not deter."[19] The dynamic between deterrence and combat capability eases when prioritizing focus. Emphasis for global strike forces should first be on the ability "to hold any target at risk,"[20] which is combat power projection. Indeed, "emphasizing the deterrent purpose can produce a force with less warfighting capability, which in some settings could in turn undercut deterrence."[21] *The secondary effect of correct combat vitality may be a deterrence effect but it cannot be the other way around.* Hence, prioritizing a global force on deterrence over combat power may fall short of capability in both. This can lead to numerous issues, from inefficient operations tempo, to cultural problems.

Cultural Implications of Deterrence Strategy

Global strike commanders are aware that at any time their unit may have to conduct global combat operations in order to meet national security strategy objectives. An abstract vision or mission of deterrence can breed a culture where leaders posture the home-base peacetime operations tempo similar to conducting combat operations. This phenomenon, called "deployed in garrison," literally applies to intercontinental ballistic missile (ICBM) operators when sitting alert, as they are "deployed," ready to launch. It also relates to many other communities in the DoD, such as remotely piloted aircraft operators engaged in daily warfare. However, it is not an accurate categorization for the bomber community. This is where the challenges of leading and maintaining a global strike force, which must be constantly ready for any possible operation, emerge. If deterrence is ambiguous, thus the operational tempo becomes similarly ambiguous. AFGSC personnel and assets are at risk of vigorously sustaining an unsustainable operational tempo and it may be, in part, due to the priority of deterrence over combat capability. The other variable is in the methodologies of how a global strike force tackles the challenge of being ready for anything, anytime.

AFGSC assets currently are in phase zero or phase one of operations plans, where the goal is to shape or deter the security landscape under peacetime conditions.[22] Many plans are developed to the highest levels of readiness next to an actual war order. In the joint plans domain, this is called a level 4 plan, where the forces, support assets, and concept of operations are already identified.[23] Bomber units must be ready to deploy from stateside bases, if those plans are executed. Yet, stateside bombers are *not* deployed, hence a more accurate categorization of bomber readiness is

---

19. Lt Col. Charles M. Westehnhoff, "Military Air Power: The Cadre Digest of Air Power Opinions and Thoughts," *Airpower Research Institute*, Air Univeristy Press, Maxwell AFB, AL, October 1990, 44, http://www.au.af.mil/au/awc/awcgate/au/westenhoff_milquote_1990.pdf.

20. James and Welsh, "Fiscal Year 2015 Air Force Posture Statement," 17.

21. Butterworth, "Nuclear Force Planning: Odin or Onan?," 12.

22. Joint Publication (JP 3-0), *Joint Operation Planning* (Ft. Belvoir, VA: Defense Technical Information Center, 2011), v6, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

23. Ibid., II–24.

"postured in place." This means bombers maintain a level of readiness to respond to any global contingency or operations plan, within a certain time.

This poses a challenge to keeping forces rested and motivated, when they are asked to be constantly ready for combat, yet live under peacetime conditions. To successfully overcome this challenge, personnel need to see the results and validity of the capabilities they train to. The paradox is that AFGSC operators are charged with carrying out the deterrence mission to such an effective level that they may never see combat. This cultural challenge is unique to AFGSC, in the sense that there are no others tasked with executing dual doctrine missions from stateside bases. The absence of conflict (i.e., deterrence effectiveness) does not fully motivate global strike operators, or build combat proficiency. However, testing their combat capability against a twenty-first century threat would both motivate and build proficiency.

Twenty-First Century Readiness Recommendations

Simply possessing a weapons system does not deter. Achieving comprehensive combat capability requires merging a weapons system with a highly intelligent and capable human operator. The final evolutionary step is to build an exercise that validates deterrence posture through *proven combat capability*. The Air Force does this through multiple exercises in the conventional realm, but requires advancements in integrating the nuclear mission. Currently, there is no holistic method to test integrated nuclear and conventional combat capability against a twenty-first century threat environment.

The Schlesinger Report concluded, "operational readiness should be measured through a comprehensive, end-to-end simulation of force employment, beginning with mission planning and concluding with *mission execution*."[24] Currently, the Air Force uses overlapping methods to adhere to that requirement.

Recommendation One: Combine Nuclear Exercises

Scenario-based drills are essential to the proficiency of securely moving nuclear assets into a heightened posture. For the past several years, USSTRATCOM and AFGSC have conducted biannual nuclear exercises where bombers, ICBMs, and intelligence surveillance and reconnaissance (ISR) assets exercise nuclear posturing. However, beyond the ground movement of weapons, nuclear exercises do not always conclude with mission execution, which means integrating with other players, employing practice bombs, in a threat scenario. At times fly-offs of bombers are carried out, but those missions rarely include inert training weapons or execution within a joint force. The lack of a true life-cycle mission—from scenario development, to mission planning, to weapons movement, to alert, launch, and bombs on target in a threat environment—equates to a mission set not validated as combat effective against the backdrop of the twenty-first century threats.

Parallel in intent, but separate from nuclear exercises, aircrews conduct nuclear weapon system evaluation programs (WSEPs). Ironically, neither USSTRATCOM nor AFGSC own these programs. Moreover, the objectives are nearly identical to nuclear exercises: to evaluate the life cycle of a

24. Schlesinger, *Phase II, Review of the DoD Nuclear Mission*, 32.

nuclear weapon from construction to employment. Only one or two crews execute these missions at a time and, reiterating again, absent a threat scenario. However, they do have the mission execution (i.e., bombs over target) piece of the life cycle cited in the Schlesinger Report. Additionally, the most important perspective to maintain is the role of training versus evaluation. To innovate and validate future nuclear combat capability, personnel must be allowed to train. Constant evaluation, without allowing time for training, prevents growth and improvement. Through training, the human weapons system can be allowed to practice, make mistakes, learn, and ultimately progress. It is possible to efficiently streamline these analogous practices to holistically validate capability.

The most efficient manner of proving combat capability is to create an all-encompassing exercise that molds the WSEP mission with USSTRATCOM exercises. In remembering that validation of combat capability, not deterrence, is a key motivator, global strike operators must be able to comprehensively dry-run what they may be called to execute. This process builds combat effectiveness, which in turn shapes deterrence credibility, fulfilling Schelling's goal, which is that "we have learned that a threat has to be credible to be efficacious."[25] This simultaneously demonstrates resolve, which is done only through practice, and showcasing that practice, of capability.[26] Moreover, streamlining exercises eases operational tempo.

Restructuring operational focus into specialties is designed to overcome ambiguity in deterrence theory. Due to the demand for global preparedness present throughout national security strategy documents, the operational bomber force has only a generalized level of proficiency in numerous areas and no supreme expertise in specific areas. The strategic demands of the twenty-first century mandates that operators attain extremely high proficiency and "think deeply and strategically."[27] Streamlining priorities and dividing tasks would result in the specialized skills needed.

Recommendation Two: Regionally Align Bomber Squadron Missions and Training

When an organization has a monumental task, requiring supremely high standards of global performance, it divides tasks. It is unsustainable to expect all personnel to maintain a high level of proficiency in all global mission areas. Bomber aircrew members must be familiar with multiple areas of responsibility (AORs), hundreds of threat systems, and numerous scenarios. The battle of balancing multiple training priorities, can result in limited or varying levels of proficiency, and even degraded morale. Moreover, as true throughout the DoD, the bomber force does not possess unlimited resources or personnel. Hence, the force may need to specialize, with a concentration on building true holistic experts in prioritized areas. As the Army and Navy have discovered, this does not hurt overall global responsiveness, but in fact increases it. Through divided specialization, AFGSC can drastically improve global capabilities, while remotivating personnel and relieving operational tempo stress.

---

25. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), 6.

26. David Santoro and Brad Glosserman, "Healey Is Wrong: Its Deterrence, Stupid," *War on the Rocks*, October 14, 2016.

27. Moon, "STRATCOM Commander Addresses Strategic Deterrence in 21st Century."

Paralleling the strategic demands of AFGSC in some form, the Army has recognized comparable challenges in global preparedness and has chosen to tackle the problem through building a doctrine of regional alignment.[28] At the brigade level, leaders assign a brigade combat team (BCT) to a specific AOR. The BCT now has a focused training and posturing priority, streamlining time and people to be lethal against a specific target set. By allowing soldiers to focus on their operational environment, the Army's overall combat readiness and global responsiveness to any AOR improved.[29] The Navy takes a similar approach, as carrier battle groups are assigned to certain geographic areas, giving those sailors a clear strategic vector and training priority.

AFGSC's holistic strategic capability may increase by dividing priority among the force. Specialization can result by assigning each bomber wing a number of AORs to divide among its squadrons. This already takes place, in some form, when a deployed bomber unit is in a specific region. For example, when a squadron of B-52s is on station at Guam, there is little reason for the remaining stateside B-52s to apply the same training weight of effort to that AOR, depending on the global security condition.

Specialization has numerous secondary effects. First, commanders can build a specific vector for training personnel. Tailored airframe training regulations, written to focus on a specific AOR, build subject matter experts (SMEs) in theory and tactical employment, both of which are requirements for twenty-first century conflict. A unit would maintain this focus for a set time and then the rotations would shift, thus giving an operator increased training in numerous AORs. The overall results are bomber units and aircrew who can attain much higher levels of proficiency.

The number of bombers available is an initial limitation to this concept. In the early 1990s, with hundreds of bombers in inventory, this methodology was easier. The solution today is to build the training focus around numbers of people, not aircraft. This will fulfill the strategic requirement of specialized and focused skill sets expertise, without the critical reliance on asset metrics. Many of the baseline tactical and strategic skills used by bomber aircrew against one area are still transferable to another. The Army discovered this concept to be true during research on how to specialize the BCTs.[30] For example, if certain units are true SMEs at taking apart a specific country's air defenses, those same advanced-level skills can increase their abilities in a different scenario. Moreover, the unit with specialized training can fight *immediately,* allowing for a faster response timeline, thereby bolstering the postured-in-place capability. Because the priority focus is clear, combat power has increased while reducing the strain on personnel. The force can meet the demands of the QDR *anywhere, anytime* more efficiently.

The glue between all these variables is not simply structure or focus. Ultimately, people are the critical piece to the success of future combat operations.

---

28. Association of the United States Army, "Regionally Aligned Forces and Global Engagement," 2013 AUSA Conference, accessed March 1, 2017, http://www1.ausa.org/meetings/2013/AnnualMeeting/Documents/Presentation_RegionallyAlignedForcesAnd%20Global%20Engagement.pdf

29. Michael C. Flynn, "Preparing for the Future: The Regional Alignment of U.S. Army Brigade Combat Teams" (master's thesis, U.S. Army Command and General Staff College, Leavenworth, Kansas, 2013), 47–49.

30. Ibid., 93.

BUILDING A TWENTY-FIRST CENTURY HUMAN WEAPONS SYSTEM

> When we commit America's sons and daughters into combat, we must ensure that they are the best-trained, best-equipped, and best-led fighting force on the planet. That takes time, it takes money, and it is perishable.
>
> –General Martin Dempsey, Chairman, Joint Chiefs of Staff[31]

In the words of Chuck Hagel, former secretary of defense, "the quality of military people is the most critical element of the defense enterprise."[32] The Air Force's recent 2020–2030 vision document clearly outlines the resources needed to meet future strategic demands. However, there is no mention of specific innovations relating to the development of people.[33]

Millennials entering the workforce have "a very different way of thinking, about their careers, about choice, about what excites them," stated former secretary of defense Ash Carter.[34] Variables, such as the increasing time demand upon men and women to raise their children, require the branches of the U.S. Armed Forces to develop and present a plan of how they are going to provide the needed stability to families while simultaneously meeting the demands of global preparedness. Additionally, military personnel today are more educated than ever before.[35] Military millennials are more likely to have a spouse who has a college degree and a career, thus changing their vocation calculus significantly.[36] Currently, there is no career plan that systematically considers all these emerging variables.

The previous analysis of future deterrence and readiness levels leads to numerous conclusions as to the specific investments needed in global strike airmen. The crucial first step is to understand that a centralized DoD personnel system is not the solution; it is the problem.[37] Recently, former Secretary of Defense Carter initiated human resource reforms not seen since the National Defense Act of 1947.[38] This revolution is long overdue and the DoD must take on a generational perspective when enacting change. Some key factors that determined why the officers decide to stay in or

---

31. DoD, *Quadrennial Defense Review 2014*, 64.

32. Amaani Lyle, "Hagel Lauds Nuclear Enterprise Airmen as 'Indispensable' in National Security," *DoD News*, November 14, 2014, http://www.defense.gov/news/newsarticle.aspx?id=123642.

33. John A. Shaud and Adam B. Lowther, "An Air Force Strategic Vision for 2020–2030," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 8–31, http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf.

34. Anna Mulrine, "For Military Millennials, 'Duty or Child?' Is Not Just an Issue for Women," *Christian Science Monitor*, April 4, 2015, http://www.csmonitor.com/USA/Military/2015/0404/For-military-Millennials-duty-or-child-is-not-just-an-issue-for-women.

35. Ibid.

36. Ibid.

37. Tim Kane, *Bleeding Talent* (New York: Palgrave Macmillan, 2012), 10.

38. Andrew Tilghman, "Pentagon's Quiet Push for Military Personnel Reform," *Military Times*, May 11, 2015, http://www.militarytimes.com/story/military/pentagon/2015/05/11/personnel-reform-push/70895094/.

leave this all-volunteer force are "organizational inflexibility, primarily manifested in the personnel system," and, specifically, the "limited ability to control their own careers."[39]

The latest extensive change to military management was through the 1986 Goldwater-Nichols Act, yet it was unsuccessful at revolutionizing the personnel system. Additionally, it also failed to "standardize training or evaluation" of personnel within the nuclear enterprise.[40] Each DoD community has specialized skills and thus requires specialized training and management. Former Defense Secretary Carter understood this, and recognized that "modernizing the personnel system may require creating unique rules for specific career fields."[41] This is especially true for a 24/7 deterrence force. Bomber career fields, require a foundation of tactical proficiency as well as abilities in critical thinking, deterrence educationand knowledge of how to lead a postured-in-place force. While some of these elements already exist, they do so under the adage of a generalized focus.

Recommendation Three: Build a Career Roadmap Tailored toward Global Strike Personnel

Culture within the DoD is ripe for change. AFGSC should capitalize on the momentum and create a roadmap for global strike personnel. As of the fall of 2015, Acting Undersecretary of Defense for Personnel and Readiness Brad Carson is leading the DoD in molding the human resource system into a "force of the future."[42] There are numerous positive outcomes to AFGSC taking the lead on how it builds its force for the future. First, it allows AFGSC to dictate how to groom its personnel. Second, a roadmap provides a recruitment and retention tool by outlining the opportunities and experiences expected during an Air Force career. Third, if built correctly, it can deliver more predictability for the next generation of airmen and their families.

Future AFGSC aircrew should have training and experience in multiple airframes. AFGSC's Striker Vista program now incorporates exchange tours between bombers for pilots and navigators will enable the mastery of technical, tactical, and strategic skill sets, thus bolstering combat capability. This process serves to strengthen the force by allowing for diversity of thought and experience. Young pilots and navigators starting their Air Force undergraduate training will seek out AFGSC assets if they know they will have the opportunity to employ multiple platforms.

Culture and Language Specialization

If the requirement directed by national security doctrine is to be a true global force, ready to deter and fight in any AOR, any time, then global strike planners and tacticians must possess intimate working knowledge of those AORs. In order to gain such knowledge, personnel need to be leaders who can "assume the mantle as the geopolitical landscape continues to change."[43] Additionally, AOR staff headquarters require global strike personnel be comprehensively integrated within the

39. Kane, *Bleeding Talent*, 102–103.

40. Kristen Goodwin, "Nuclear Command, Control, and Communication: Strengthening a Neglected, but Critical, Component of the U.S. Deterrent," *Nuclear Notes* 3, no. 1 (August 2013): 12.

41. Tilghman, "Pentagon's Quiet Push for Military Personnel Reform."

42. Joe Gould, "DoD Personnel Official Rips Outdated Personnel System," *Defense News*, June 24, 2015.

43. Moon, "STRATCOM Commander Addresses Strategic Deterrence in 21st Century."

joint planning process. The Schlesinger Report highlighted the deficiency of nuclear and global strike experience throughout the combatant commands, and the deficiency remains.[44] The Air Force tackled this issue by thinking about personnel through the old centralized methodology. Key nuclear billets (KNBs) were created (a code all nuclear personnel receive) with the intent to manage nuclear personnel into certain areas. Instead, the opposite effect happened, as commanders could not send the right people to the right areas if there were no KNB slots available.[45]

Warden and Boyd both recognized that for a strategy to work, personnel must be able to understand and overcome cultural barriers.[46] Without comprehensive knowledge of an enemy, beyond simply the locations of threats and targets, the full-spectrum of warfare—including cultural, economic, and political elements—is incomplete. Linking members of a specific AOR-focused bomber unit to a specialized career roadmap allows the necessary talents to fall into place. Immersion, both academically and physically in the AOR of specialty, should be part of this process. This results in exponentially greater combat effectiveness and deterrence capability. Language capacity, for example, is currently in extreme demand in the field, yet there is a limited supply of qualified personnel.[47] This would not be the case if the personnel system reflected operational requirements. Moreover, because future operational demands are going to require further specialization, the personnel system must be built to attain and reward such development.

Beyond cultural skills, AFGSC personnel need critical leadership training throughout key points in their career. This training must focus on the unique challenges faced by AFGSC leaders when commanding a globally postured-in-place, dual doctrine combat force.

Leadership and Education

Professional education and leadership training courses should not exist as stand-alone events. Instead, by ingraining leadership training into a specialized career path roadmap, a comprehensive methodology that is deliberately designed for global strike is built and personnel are fully prepared for future combat. Personnel must receive this holistic training from day one of their careers.

A global deterrence force presents unique leadership challenges. In theory, the mission of a deterrence force is to train so well and be so deadly that it never has to go to combat. Arguably, the psychology of this dilemma from a perspective of how to lead such a force remains misunderstood. There are lingering cultural challenges within the nuclear force structure. One such challenge is the fact that there may be numerous commanders and leaders at various levels with no combat experience. The B-2 community has not seen, extended combat in almost a decade. After a nine-year hiatus, the B-52 community has recently seen action in Syria. The ICBM community is unique, in that commanders will never have combat time. For those who have seen combat, it has only been in a largely permissive environment. Yet, the force is expected to be ready for the next

44. Schlesinger, *Phase II, Review of the DoD Nuclear Mission*, 17.

45. USAF colonel, interviewed by the author, May 6, 2015, under conditions of nonattribution.

46. Stephens, "Fifth Generation Strategy," 134.

47. Kane, *Bleeding Talent*, 126.

generation fight, consisting of a significantly non-permissive and area denial environment.[48] As officers grow throughout their career, experiences consist of training and posturing under a deterrence mind-set, not employment in actual combat.

Scholars, commanders, and policymakers must realize that this nation has allowed the quality of thinking about nuclear deterrence "to reach a dangerously low level."[49] AFGSC has undertaken numerous measures to address this issue. First, exposure to both nuclear operations and global dual doctrine deterrence strategies within broader Air Force educational and training programs is taking place. The Air Force is pushing educational opportunities through a number of military and private organizations. AFGSC is integrating with civilian programs like the Center for Assurance, Deterrence, Escalation, and Nonproliferation Science and Education (CADENCE) at Louisiana Technical College. These are important first steps.

AFGSC has developed the Nuclear Leadership Development Center (NDLC). The NLDC has set out to develop and impact global strike practitioners *before* they experience the next level of needed leadership. Beyond USAF formal developmental education programs, the NLDC will have the specialized cadre and syllabus to address the unique cultural challenges present within a global strike force.

The NLDC is integrated with groundbreaking programs already present at the USAF Academy, such as the Center for Character and Leadership Development (CCLD), whose stated mission is to "advance the understanding, practice, and integration of character and leadership development."[50] Additionally, Air Education and Training Command has developed the Profession of Arms Center of Excellence (PACE), which is working in parallel with NDLC cadre to ensure the specialization of leadership training for global strike forces is comprehensive and effective. PACE and CCLD have a strong focus on character development, while the NDLC can build on that foundation and mold it into the training required to address the needs of a global strike force. Necessary topics are the proper application of force readiness, the priority of people versus the mission and the character and leadership development of the human weapons system.

CONCLUSION

The 2014 Quadrennial Defense Review stated that "innovation is the military imperative and the leadership opportunity of this generation . . . it's a fleeting opportunity."[51] Global strike methodologies are improving, but dual doctrine theory still has numerous entanglements in Cold War–era thought. During the twenty-first century, that will have to change. "If western strategic thinking is to progress, experience indicates it is time for a different military culture."[52] The global strike force

48. Robbie Gramer and Rachel Rizzo, "China's Maginot Line," *War on the Rocks*, August 11, 2015.

49. Paul J. Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (New York: Henry Holt, 2012), 217.

50. Center for Character and Leadership Development, United States Air Force Academy, accessed May 11, 2015, http://www.usafa.edu/Commandant/cwc/index.cfm?catname=cwc.

51. DoD, *Quadrennial Defense Review 2014*, 64.

52. Stephens, "Fifth Generation Strategy," 155.

has neither the time nor resources to maintain the status quo of generalized specialization if it is going to achieve the strategic demands of the nation in an efficient way. Maintaining the priority focus on deterrence shifts the culture into a realm that is abstract and in reality hurts combat capability. When combat power is the priority focus, it quickly becomes evident that there are superior and more efficient ways to accomplish the mission. Most importantly, focusing on combat power first can ultimately increase the military deterrence, hence overall strategic deterrence and national security posture. If the force trains to win, a strong deterrence effect will naturally follow.

Nuclear Command and Control in the Twenty-First Century: Maintaining Surety in Outer Space and Cyberspace

Jared Dunnmon[1]

Cyber vulnerabilities in the space-based component of U.S. nuclear command, control, and communications (NC3) systems represent a significant risk to ensuring continuing nuclear stability. This paper examines emerging threats to the surety of the U.S. nuclear deterrent resulting from asymmetric threats to space-based assets from actors in the cyber domain, and considers how responses to such threats could be framed in terms of the laws of armed conflict. Several scenarios are developed to demonstrate both the immediacy and the inherent difficulty of operational problems that could result from current NC3 architectures. Finally, distinct sets of recommendations spanning both technology and policy domains are developed with the goal of reducing the possibility of nuclear destabilization caused by a cyber attack on U.S. NC3.

---

1. Jared Dunnmon is a PhD candidate in engineering at Stanford University. His academic interests encompass energy and propulsion systems, artificial intelligence, nuclear deterrence, and improving cyber-physical resilience in critical infrastructure systems. In addition to his research work, Dunnmon is affiliated with the Stanford Hacking for Defense (H4D) project, focused on applying Silicon Valley rapid innovation techniques to pressing problems in defense and national security. Dunnmon holds a bachelor's degree in mechanical engineering from Duke University in addition to master's degrees in both scientific computing and business administration from Oxford University. This manuscript would not have been possible without the support, time, and effort of a wide variety of individuals. The author would especially like to thank Ambassador Linton Brooks, Dr. James Miller, Dr. John Harvey, Dr. James A. Lewis, Professor Scott Sagan, Admiral James O. Ellis, Dr. Herbert Lin, and Mallory Stewart for their engagement during this project.

INTRODUCTION

In the years following the conclusion of the Cold War, the nature of international nuclear dynamics has fundamentally changed. Instead of a nuclear community dominated by mutually assured destruction between two superpowers, the last several decades have seen proliferation of nuclear capabilities in new locations such as Iran and North Korea combined with unprecedented democratization of powerful technology previously confined to nation-states.[2] In particular, the rapid global uptake of high-performance computational capability, reduced barriers to space access, and widespread proliferation of knowledge via the Internet have eroded many of the technological advantages previously held by nation-states.[3]

The challenges associated with these new realities are particularly important in the ongoing process of ensuring the security and strategic stability of the U.S. nuclear deterrent through the nuclear command, control, and communications (NC3) system. The purpose of the NC3 system is to link nuclear forces to presidential authority; this is accomplished via a complex system that includes space-borne and terrestrial early warning radar, facilities to interpret early warning information, various terrestrial and airborne command and control posts, and communications infrastructure comprised of satellite, radio frequency (RF), and land-line communications.[4] As noted by Admiral Cecil Haney in his capacity as United States Strategic Command (USSTRATCOM) commander, "Assured and reliable NC3 is critical to the credibility of our nuclear deterrent. The aging NC3 system continues to meet its intended purpose, but risk to mission success is increasing. Our challenges include operating aging legacy systems and addressing risks associated with today's digital security environment."[5]

Much of Admiral Haney's testimony focuses on the specter of threats in the cyber domain, the full definition of which can be succinctly stated as "an operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and internetted information systems and their associated infrastructure."[6] This emphasis on cyber threats to NC3 systems echoes conclusions of both the Defense Science Board[7] and the 2014 Quadrennial Defense Review (QDR).[8] In addition, a variety

2. George P. Shultz, William J. Perry, Henry A. Kissinger, and Sam Nunn, "A World Free of Nuclear Weapons," *Wall Street Journal*, January 4, 2007.

3. Jason Fritz, "Hacking Nuclear Command and Control," International Commission on Nuclear Nonproliferation and Disarmament, 2009, http://icnnd.org/documents/jason_fritz_hacking_nc2.doc.

4. John Harvey, "Nuclear Command and Control for the 21st Century" (speech given at the DNUG Conference, September 23, 2014, Lorton, VA).

5. Senate Committee on Armed Services, "Statement of Admiral C. D. Haney, Commander, United States Strategic Command," 113th Cong., 2nd sess., February 27, 2014, 9.

6. Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin Kramer, Stuart Starr, and Larry Wentz (Dulles, VA: Potomac Books, 2009).

7. Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2013).

8. U.S. Department of Defense (DoD), *Quadrennial Defense Review Report, 2014* (Washington, DC: DoD, March 2014).

of scholars have described the dire consequences of an NC3 architecture compromised by cyber incursion, including false alarms, inadvertent launches, loss of contact with nuclear weapons, premature detonation, and a fundamental loss of nuclear strategic stability.[9] It is therefore imperative for global safety and security that NC3 systems be safeguarded from cyber intrusion.

Unfortunately, given the increasingly complex nature of the NC3 systems described above, there exist a variety of potential attack vectors that could be exploited by malicious interests, including both state and non-state actors. Such attacks could be categorized as follows: communicating inaccurate actions or intentions, increasing perceived time pressures to act or respond, disrupting or destroying communications channels, and hindering the search for viable alternatives.[10] For effective NC3 operation, for instance, it is crucial that early warning sensors give accurate information on whether another state has launched a nuclear attack; otherwise, erroneous assessments could result in an unintended nuclear exchange. Ambiguity in early warning systems is particularly problematic given that watch personnel generally have only three minutes to initially differentiate a nuclear launch from such mundane events as solar reflection off the water, wildfires, and ever more common commercial satellite launches.[11]

Effective NC3 operation is also directly reliant on assured communications between key elements of leadership. Specifically, the minimum essential electronic communications network (MEECN) represents the critical linkage between presidential authority and the three legs of the command, control, and communications triad. This system includes airborne (E-6B TACAMO, E-4B NAOC, B-52 bomber), satellite (AFSATCOM, MILSTAR, AEHF), seaborne (SSBN), and ground-based (NMCC, MRT) assets. Disruption of this communications network would erode or neutralize U.S. capability to rapidly execute decisions made by strategic leaders.[12]

Finally, reduction in the number of viable nuclear response alternatives detracts from strategic stability. If part of the nuclear enterprise (e.g., any leg of the command, control, and communications triad, or a component of the NC3 system) is believed to have been compromised by an adversary, it becomes much more likely that any further perceived aggression will be met with nuclear response.[13] In the end, it is clear that any degradation of the U.S. NC3 system materially increases the possibility of nuclear conflict and the associated human catastrophe. It thus remains imperative that vulnerabilities to this architecture be minimized.

---

9. Andrew Futter, "Hacking the Bomb: Nuclear Weapons in the Cyber Age" (paper presented at the ISA Annual Conference, New Orleans, LA, February 2015); Eric Schlosser, *Command and Control: Nuclear Weapons, The Damascus Accident, and the Illusion of Safety* (New York: Penguin, 2013); Bruce Blair, "Rogue States: Nuclear Red Herrings," *Defense Monitor*, January 2004; Richard J. Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* (Washington, DC: Center for New American Security, 2014).

10. Futter, "Hacking the Bomb."

11. Blair, "Rogue States."

12. Fritz, "Hacking Nuclear Command and Control." AEHF, Advanced Extremely High Frequency; AFSATCOM, Air Force Satellite Communications; MILSTAR, Military Strategic and Tactical Relay; MRT, Miniature Receive Terminal; NAOC, National Airborne Operations Center; NMCC, National Military Command Center; SSBN, strategic ballistic missile submarine.

13. Futter, "Hacking the Bomb."

This paper will first present an overview of how the democratization of key technologies in the early twenty-first century has led to the development of asymmetric threats to NC3 systems in the space and cyber domains. Next, it will consider how the traditional laws of armed conflict could be adapted to the cyber domain within the context of its interaction with NC3. Analysis then proceeds to consider two different scenarios to demonstrate how the combination of asymmetric threats, current NC3 technology, and ambiguous laws of armed cyber-conflict could put U.S. leadership in difficult strategic decisionmaking situations. Finally, the discussion concludes with a set of technical and policy recommendations intended to reduce the possibility that such scenarios would ever come to pass.

ASYMMETRIC THREATS TO NC3 IN THE TWENTY-FIRST CENTURY

While rapid advances in information technology, communications, and computation have yielded many improvements to NC3 systems, these improvements have come at the cost of NC3 surety and security. The two domains in which these costs are most apparent are the two newest arenas of conflict: outer space and cyberspace. In the words of Admiral Haney, "the space domain, along with cyberspace, is simultaneously more critical to all U.S. operations yet more vulnerable than ever to hostile actions."[14] The worrisome combination of international norms that have been far outpaced by the speed of technological advancement and democratization of key space and cyber technologies has led the United States to a point where it is difficult to be confident that the current NC3 structure is resilient in a cyber-physical sense.

Outer Space

The major threat to NC3 posed by vulnerabilities in space-based assets results from potential disruptions to both early warning and communications functions. As noted by Frank Rose, former deputy assistant secretary of state for defense policy and verification operations,

> The United States in particular is deeply reliant upon space. While such reliance enables the United States and our allies and partners to undertake a range of operations in support of peace and security, this reliance has increasingly been viewed by potential adversaries as a vulnerability to be exploited through the development of counterspace capabilities.[15]

This reality is particularly emergent in the context of NC3. At present, it is known that Russia and China are actively pursuing or already maintain such capabilities as laser weapons for satellite denial,[16] electromagnetic (EM) jamming for communications degradation, and physical antisatellite

14. Senate Committee on Armed Services, "Statement of Admiral C. D. Haney Commander United States Strategic Command."

15. Frank Rose, "Using Diplomacy to Advance the Long-Term Sustainability and Security of the Outer Space Environment" (remarks at International Symposium on Ensuring Stable Use of Outer Space, Tokyo, March 3, 2016).

16. Ibid.

(ASAT) systems.[17] Given heavy reliance on satellites such as Advanced Extremely High Frequency (AEHF) and Air Force Satellite Communications (AFSATCOM) in the NC3 system, ensuring both reliability and resiliency to these types of threats will be critical to creating a flexible and efficient NC3 system.

Cyberspace

In the cyber domain, potential vulnerabilities exist in all three parts of the command, control, and communications triad. Specifically,

> due to cyberspace's relatively low cost of entry, cyber threats range from state-sponsored offensive military operations and espionage activities, to [violent extremist organizations] intent on disrupting our way of life, to cyber criminals and recreational hackers seeking financial gain and notoriety. Additionally, the U.S. supply chain and critical infrastructure remains vulnerable to cyber attack, and even as we detect and defeat attacks, attribution remains a significant challenge.[18]

At present, assumptions are that NC3 is secured via a combination of air gaps, technological superiority in outer space and cyberspace, and human intervention in the control loop. Unfortunately, this is not always the case. In the intercontinental ballistic missile (ICBM) program, for instance, documented vulnerabilities include potential entry into the firewalled NC3 system, phony orders being conveyed via a backup antenna, distributed denial of service (DDoS) attacks on the nuclear infrastructure, and even a direct attack on thousands of feet of cable of the Hardened Intersite Cable System.[19] For the strategic ballistic missile submarine (SSBN) component, it has been widely publicized that the United States has chosen to use Linux-based operating systems in its SSBNs, as opposed to Windows XP-based architectures currently used by the British Trident program.[20] While neither of these operating systems is inherently problematic, the fact that their use in specific functional domains has been published so widely will enable hackers to focus on the correct class of exploits to use against these systems.[21] This observation, furthermore, hints at a distressing reality: with the emergence of ubiquitous cyber threats, the U.S. acquisition process has already begun moving toward increased levels of security and classification across the Department of Defense (DoD) enterprise, which hinders efficiency at all levels of the acquisition process. Without firing a shot, the opponent may well have caused substantial cost to the United States already due to the inefficiency resultant from broadly increased data security and classification procedures.

With the bomber airborne component of the command, control, and communications triad, the Air Force has experienced several NC3 breakdowns in the past several decades, the most recent of which involved the inadvertent placement of several nuclear warheads in a strategic bomber that

17. Harvey, "Nuclear Command and Control for the 21st Century."

18. Senate Committee on Armed Services, "Statement of Admiral C. D. Haney Commander United States Strategic Command."

19. Blair, "Rogue States."

20. Futter, "Hacking the Bomb."

21. Fritz, "Hacking Nuclear Command and Control."

flew over the United States.[22] While this latter situation was not necessarily a cyber failure of commission, it is certainly one of omission in the sense that appropriate command and control safeguards were not in place to prevent such a mistake from occurring.

Critical infrastructure that either directly or indirectly supports the nuclear enterprise, such as the domestic power grid is also vulnerable to cyber attack.[23] Janet Napolitano, former secretary of homeland security, recently estimated that an adversary could disable one of the major U.S. power grids with 80 to 90 percent probability of success.[24] The frequency of such cyber vulnerabilities generally correlates with the size of the codebase—one can usually assume one error per thousand lines of code. For perspective, a generic Linux operating system had 15 million lines of code as of 2011.[25] Thus, while the National Nuclear Security Administration (NNSA) currently deploys a wide variety of cyber-defense techniques in defense of nuclear assets, including vulnerability scanning, firewalls, commercial antivirus systems, encryption, data loss prevention, data at rest security, network monitoring, enterprise forensics, and automated security control assessment, it is impractical to find every possible vulnerability in a large codebase and thus impossible to guarantee absolute security from zero-day exploits.[26] Further, post-detection attribution remains a challenge that usually takes weeks to sort out, meaning that attribution may be unachievable on timescales characteristic of a crisis.[27]

Combined Threats in Cyberspace and Outer Space

Many of the most daunting challenges for NC3 resilience lie at the intersection of cyberspace and outer space domains, where cyber attacks are directed at space-based NC3 assets. A recent study revealed substantial numbers of exploitable flaws in many widely used commercial satellite architectures, including the Iridium constellation, International Maritime Satellites (INMARSAT), and other satellites commonly used by both North Atlantic Treaty Organization (NATO) forces and critical infrastructure systems.[28] Key vulnerability categories included hard-coded credentials (undocumented credentials that can authenticate in documented interfaces), undocumented protocols (protocols not intended for end users), insecure protocols (end-user protocols that pose a security risk), and backdoors (mechanisms used to access features not intended for end users). Outcomes from reported exploits included control over systems as varied as

22. Douglas Raaberg, "Commander Directed Report of Investigation Concerning an Unauthorized Transfer of Nuclear Warheads," unclassified document, August 30 2007, available at http://scholar.harvard.edu/files/jvaynman/files/minot_afb_report.pdf.

23. Janene Scully, "VAFB Power Plant to Help During Crisis," *Lompoc Record* (Santa Maria, CA), June 4, 2001, http://lompocrecord.com/news/local/vafb-power-plant-to-help-during-crisis/article_a5129e90-46f6-5459-ad26-754a42294f52.html.

24. Ted Koppel, "How Vulnerable Is US to Cyberattack on Power Grid? Very," *News & Observer* (Raleigh, NC), November 3, 2015.

25. Danzig, *Surviving on a Diet of Poisoned Fruit*.

26. "Stockpile Stewardship Management Plan," National Nuclear Security Administration, 2016, https://nnsa.energy.gov/ourmission/managingthestockpile/ssmp.

27. James A. Lewis, personal conversation with the author.

28. Ruben Santamarta, "A Wake-up Call for SATCOM [Satellite Communications] Security," IOActive, April 17, 2014, http://blog.ioactive.com/2014/04/a-wake-up-call-for-satcom-security.html.

land-based communication and aircraft navigation, either of which could have a debilitating effect on MEECN integrity and ultimate NC3 efficacy. Understanding and mitigating the potential effects of these cyber threats to space-based assets will be imperative in ensuring the continued effectiveness of NC3.

LAWS OF ARMED CONFLICT: OLD RULES FOR NEW DOMAINS

While technical capabilities in outer space and cyberspace have continued to evolve, the laws of armed conflict have still not been updated to fully cover the new environment. Degradation of NC3 via cyber attack, with space-based assets being particularly vulnerable, can have a debilitating impact on the credibility of the nuclear deterrent. Even one successful cyber attack could have devastating consequences for global stability. As has been widely chronicled, the cyber domain poses unique difficulties to traditional application of conventional laws of armed conflict.[29] Such challenges are exacerbated when nuclear systems are involved.

For instance, to maintain nuclear strategic stability, it is generally helpful that any actions happen slowly (adversaries would have time to observe an action and respond), openly (actions can be observed by all parties and accurately attributed), and symmetrically (both sides can perform similar actions, and similar actions would cause similar levels of damage). Cyber operations against NC3, however, have none of these attributes. Activation of malicious code via backdoors or undocumented credentials can occur in a matter of seconds. Cyber attacks also have the potential to cause outcomes varying from simple annoyances all the way to catastrophic failures—occasionally, the only difference is a few lines of code that are not visible to the attacked party. Further, even if it were possible to detect and analyze every protocol stored or running on an NC3 system, attribution processes are generally too slow to enable accurate response in any time shorter than a matter of days, making it possible for the United States to be victimized by a debilitating cyber attack without knowing what adversary was responsible.[30] Finally, and perhaps most disturbingly, cyber attacks are not limited to state actors. While it would most likely require sophisticated hacker teams with significant financial backing to find any vulnerabilities in NC3-specific systems,[31] increasing levels of intermingling between conventional and nuclear command, control, and communications (C3) systems (notably in the satellite domain) means that additional vulnerabilities may well have been introduced into current NC3 architectures.[32] It is even possible that unanticipated threat vectors that could be accessible to amateur hackers have already been introduced into U.S. C3 systems. Thus, these realities represent a dangerous dynamic that fundamentally weakens the stabilizing framework of mutually assured destruction.[33]

---

29. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

30. Lewis, personal conversation with the author.

31. Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*.

32. Harvey, "Nuclear Command and Control for the 21st Century"; Santamarta, "A Wake-up Call for SATCOM Security."

33. Danzig, *Surviving on a Diet of Poisoned Fruit*.

Given that many of these challenges will persist for the foreseeable future, it becomes important to consider how the United States should both deter and respond to cyber threats to NC3 systems in the context of international laws of armed conflict. Understanding these dynamics would not only elucidate specific policy challenges, but perhaps also assist in the process of formulating viable solutions to the difficult problem of credibly protecting NC3 via a combination of targeted technical development, cost-effective system deployment, and specific policy assertions. While a variety of documents exist that could be used to guide this process, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* represents a particularly appropriate framework for this analysis given that it was composed by an international group of experts (GoE) with the explicit goal of understanding how concepts of *jus ad bellum*, *jus in bello*,[34] and international humanitarian law apply to the cyber domain.[35] While the manual is not a formal statement of accepted international law and has not been broadly adopted, it represents a useful (though often nonunanimous) perspective from which to frame this discussion given its specific focus on "cyber operation[s] against a State's critical infrastructure, or a cyber attack targeting enemy command and control systems."[36]

Several key points that have particular application to NC3 are discussed here, with a particular emphasis on the interaction between the nuclear domain and cyber and space domains. Importantly, these ideas are not only considered from the U.S. point of view, but also from the standpoint of potential adversary nations who could conceivably use this framework as justification for actions taken against U.S. NC3.

Jurisdiction and Sovereign Immunity

Jurisdiction, which refers to the "authority to prescribe, enforce, and adjudicate," is allocated for cyber activities to any state "over (a) persons engaged in cyber activities in its territory, (b) cyber infrastructure located on its territory, and (c) extraterritorially, in accordance with international law." Importantly, national security threats including "any cyber operation that interferes with a state's military defensive systems (early warning radar and air defense)" constitute a valid justification for extraterritorial action. Further, the *Tallinn Manual* specifically states that "the fact that a State is capable of taking control of a piece of cyber infrastructure does not affect jurisdiction—specifically, a state can't take control of [a] commercial drone operated by another state over international waters." Logically, this should extend to satellites in the internationally accessible space domain as well.

Sovereign immunity fundamentally safeguards the right of a government to control its own systems. Specifically, "Sovereign immunity provides that assets controlled by the government of one sovereignty cannot be taken control of by another sovereignty without a violation of sovereignty—this includes vessels, aerial assets, and space assets."

---

34. *Jus ad bellum*: international law governing resort to force by States as an instrument of their foreign policy; *Jus in bello*: international law governing actions in armed conflict.

35. Scott Sagan, personal conversation with the author.

36. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

The jurisdictional and sovereign immunity arguments above indicate that any action taken against a satellite owned by a particular country would be generally prohibited outside of wartime. However, the GoE proposed several specific exceptions to this rule. First, in order to enjoy sovereign immunity, a particular platform must be *exclusively* performing government functions. In particular, the GoE makes the point that satellites with different transponders for commercial and non-commercial traffic do *not* have sovereign inviolability, meaning that countries could reasonably argue they are not violating U.S. sovereignty by interfering with satellites that perform key NC3 functions, but have other nongovernmental purposes as well.[37] Thus, even if broadly accepted, this specific portion of international law would not seem to provide a strong formulaic disincentive to cyber attacks on either dedicated NC3 communications satellites or those (e.g., AEHF) performing multiple functions including NC3. This is particularly true given that the *Talllinn Manual* only stipulates that a state should not "knowingly allow cyber infrastructure located within its territory or under its exclusive government control to execute operations harmful to another state." The question of what states should reasonably be expected to know about cyber infrastructure within their borders remains open.[38]

Responsibility

In general, a "state bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation." However, states could be shielded from sanction for cyber operations by the clause stating that "the law of state responsibility is not implicated or prohibited by acts of international law, per se. Thus, a state's responsibility for cyber espionage is not to be engaged as a matter of international law."

While cyber espionage should be differentiated from cyber reconnaissance in the sense that espionage relates only to activities performed within an enemy state, it is nonetheless unclear that insertion of malicious code within an enemy C3 system from within its own networks would constitute an act punishable under international law, even if accurately attributed. However, the *Tallinn Manual* also explicitly indicates that a state may engage in counter-hacking if faced with aggressive hacking against its own critical infrastructure. The key technical issue here is that differentiating espionage and reconnaissance from aggressive attack can be nearly impossible, and that the same code could perform both functions under different operating conditions. Thus, the idea that espionage and attack should be treated differently seems to be inconsistent in the cyber domain, wherein perfect knowledge about enemy capabilities once inside a sensitive network will never be possible. While this particular section opens many questions that are beyond the scope of this work, the key point is that responsibility considerations do not specifically provide any sort of protection to NC3 systems from cyber attack.

Use of Force

The *Tallinn Manual*'s prescriptions on the use of force also do not provide protection for NC3 systems. First, even if passwords are broken and firewalls are bypassed, it states that "cyber espionage and exploitation lacking an element of coercion do not per se violate the non-intervention

37. Ibid.

38. Ibid.

principle." Technically, it would be very difficult to differentiate coercion from benign activity in real time. Further, the manual specifically states that encouraging or expressing support for others' activities does not cause a state to be held responsible, and, thus, while providing hacktivist groups with malware would comprise a use of force, funding them (or other forms of enabling, nontangible support) would not. Consequently, there exists little barrier in this framework to countries' funding extremely capable third parties to execute malicious cyber activities against U.S. NC3 on their behalf.[39]

Self Defense

A key consideration in the laws governing armed conflict is under what circumstances an entity is entitled to take action in self-defense. The asymmetric nature of the cyber domain has caused it to be one of the few arenas in which attacks by a non-state actor can trigger the right to self-defense.[40] Further, while a traditional school of thought has been that self-defense is only valid after an attack has been launched, the speed at which a first cyber attack would occur might obviate any chance for a response. The GoE considered this case, and strongly backed the applicability of "anticipatory self-defense" against a cyber attack. The idea behind this term is that a nation need not wait idly while enemies prepare a cyber attack; given the speed of cyber attacks, the "last window of opportunity to defend oneself" may well be before any attack has actually occurred.[41] An example given involves insertion of a logic bomb into a government's systems—however, in this case the GoE contends that this insertion does not per se represent an armed attack, and that such a determination should not only consider the consequences of the code, but also the achievability of the conditions for activation. Unfortunately, the practicality of this particular example is burdened by the fact that it is not generally possible to know the intent or inner operation of a piece of malware before time-consuming code analysis has taken place. As mentioned above, decisions regarding responses to a potential attack on nuclear systems must be made on far shorter timescales. Thus, anticipatory self-defense appears to be a particularly strong concept in support of preemptive action against prospective cyber attack on critical nuclear systems.[42]

Law of Armed Conflict

Once it has become apparent that states are in conflict, the Law of Armed Conflict (LOAC) applies to actions taken in the cyber domain. However, several aspects of the traditional LOAC require further exploration in the context of cyber attacks on NC3 systems. The question of proportionality, for instance, becomes very difficult to assess. Specifically, the LOAC states that active response to aggression should be similar in scope and magnitude, or "proportional," to the original aggression. If part of the nation's NC3 system were compromised by adversary action, however, what would be an appropriate response, particularly if no physical damage had been done? Is this considered an attack on the nuclear infrastructure, which could potentially merit a nuclear

39. Ibid.

40. Ibid.

41. Ibid.

42. Adm. James O. Ellis, personal conversation with the author.

response? While cyber attacks against adversaries would be permitted as a proportional response, would even proportional U.S. action against enemy NC3 systems cause escalation toward nuclear conflict? How should this risk be managed? For perspective, for a time it was Russian policy to respond to strategic cyber attack with the choice of any strategic weapon in its arsenal.[43] Finally, how does the United States consider attacks on systems that perform both conventional and nuclear C3 functions, such as AEHF satellites? Would a response from any element of the military be appropriate given the possibility of an implied nuclear threat? Each of these is an unanswered question that requires a nuanced response in the context of relevant technology and policy. The *Tallinn Manual* represents a good start in addressing many of these issues, but much work remains.

A TOUGH CONFLUENCE: PLAUSIBLE SCENARIOS, DIFFICULT DECISIONS

To bring an aspect of concreteness to the analyses above, it is helpful to consider two separate scenarios where cyber operations involving the space-based portion of NC3 are compromised. Each of these is purely hypothetical, but grounded in technical reality. Further, while the analysis presented here does not propose command-level solutions to these difficult problems, the goal will be to present difficult situations that remain possible today, but could be reduced in probability by a combination of technology and policy strategies outlined in a later section.

Malware Discovery: Is the United States at War?

First, consider a scenario where a piece of malware is found on a Military Satellite Communications (MILSATCOM) satellite involved in both conventional and nuclear C3. It is unclear what state of armed conflict the United States should consider itself to be in. Is this the lead-up to an attack (*jus ad bellum)?* Is this actually an attack (*jus in bello*)? Did this software originate from a non-state actor, and thus neither of the above would apply?

Given this uncertainty, the code is analyzed, and over the next several weeks it is determined that while the malicious code is exfiltrating data to some particular nation-state with 80 percent probability, it is not affecting system operability. In this case, how should the United States respond? There are several key issues and questions to consider, none of which has a particularly easy answer or solution:

1. During the time between discovery and analysis completion, it is impossible for the United States to know whether the malicious code has the capability to disable key NC3 functions in addition to simply exfiltrating data.
2. During the interval between discovery and tentative attribution, the United States would not have visibility into what type of actor has infiltrated the NC3 system (state or non-state), and further would be unable to take an appropriately specific defensive posture toward the potential attacker.

43. Futter, "Hacking the Bomb."

3. Under international law, it is unclear if 80 percent probability is sufficient to justify assignation of responsibility.
4. It is possible that this is not the only piece of malware affecting the NC3 system. Discovery is by no means perfect, and other, more damaging codes could exist.
5. Given the above uncertainty regarding espionage versus attack, and assuming the attribution is correct, what would be an appropriate proportional response? Though these actions do not necessarily demonstrate intent to disrupt nuclear operations given the combination of conventional and nuclear C3, they could nevertheless be a prelude to nuclear attack or nuclear coercion (in a conventional conflict).
6. The United States could consider developing internal tools to disrupt an opponent's NC3 (if it exists), but this could be counterproductive. For instance, snippets of the Stuxnet code—speculated to have been developed jointly by the United States and Israel to attack Iranian nuclear capabilities—have begun showing up in other parties' attack code. This situation illustrates how the United States' own offensive cyber tools can be repurposed in opposition to the national interest. In fact, dissection of U.S.-developed anti-NC3 codes by the adversary could well provide the insights a malicious party would need to greatly harm U.S. assets. Further, as far as Russia is concerned, even U.S. development of technology to interfere with NC3 is seen as inherently destabilizing; such considerations must necessarily play into decisions about whether tools to disrupt an opponent's NC3 should be developed.[44]
7. What is standard procedure for ensuring that NC3 is not compromised in the aftermath of a potentially malicious software activation? Should an event like this be disclosed to an international legal body? What steps can be taken to ensure that other parties do not attempt to take advantage of the fact that U.S. systems may be compromised?
8. Should anticipatory self-defense remain an option in such a scenario?

The Regional Scenario: Is the United States Fighting a Nuclear or Conventional War?

We now propose a scenario wherein the United States is involved in a conventional regional conflict with a peer nuclear power. Several recent studies have, for instance, explored the possibility either of a Russian attempt to annex the Baltic states or of a Chinese attempt at territorial expansion in the South China Sea.[45] In the course of such a conventional conflict, consider the set of issues and questions that would arise if a U.S. AEHF communications satellite suddenly ceased functioning:[46]

---

44. Lewis, personal conversation with the author.

45. David Shalpak and Michael Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics* (Santa Monica, CA: RAND, 2016); Bonnie S. Glaser, "Armed Clash in the South China Sea," Contingency Planning Memorandum No. 14, Council on Foreign Relations, April 2012, http://www.cfr.org/asia-and-pacific/armed-clash-south-china-sea/p27883.

46. Ellis, personal conversation with the author.

1. What are the consequences of a relatively important node in the communications network no longer functioning? Can this node be compensated for? How long would it take to replace?
2. Did the satellite simply malfunction, or was it attacked?
3. If it was a malfunction, is this a systemic issue with the AEHF constellation or an isolated incident?
4. If it was an attack, who was the aggressor, and what was the method of the attack? If this was a physical attack, what was the mechanism? If there are co-orbital objects moving, are they passive debris or an active enemy weapons system?
5. If this was a cyber attack, are other systems compromised or are other AEHF satellites at risk?
6. If this was an attack, was the goal to attack conventional or nuclear C3? Was the opponent attempting to degrade U.S. nuclear deterrent capability? Or was it a patriotic hacker attempting to stop conventional artillery fire near his hometown? How could the United States tell one of these situations from the other? Would it and should it matter in formulating a response?

NEXT STEPS: MOVING FROM PROBLEMS TO SOLUTIONS

One approach to the above scenarios would be an in-depth analysis of each question to determine exactly how the United States should respond. However, in light of substantial modernization to the NC3 system currently planned and under way, it is perhaps most useful to consider technological and policy avenues that could be pursued with the goal of ensuring that the above scenarios, each of which is fraught with uncertainty around nuclear intentions and appropriate U.S. response, would never come to pass. Distinct sets of technology and policy recommendations intended to inform discussion around modernization and design of the future nuclear enterprise are presented below.

Technological Directions

Several concrete technological initiatives would help reduce operational uncertainty and ensure resilient NC3 functionality.

Apply Advanced Forensics Techniques

All NC3 satellites should be outfitted with advanced forensics capability. Motion sensors, heat sensors, and EM intensity sensors should be emplaced in order to assess whether any given satellite inoperability resulted from external physical attack.[47] For protection from cyber attack, domestic control over supply chains should be pursued to reduce the possibility of backdoors, insecure or undocumented protocols, and hard-coded credentials. Finally, in addition to traditional antivirus scans of satellite software, commercially available assessments based on computationally efficient

47. Ibid.

code-level machine learning tools that proactively detect both new variants and repackaged versions of existing malware should be implemented.[48] Such methods should prove powerful in reducing the possibility of a successful cyber attack on NC3 systems.

Emphasize Modern Network Defense Techniques in NC3

Traditionally, network defense has focused on keeping attackers outside of a virtual "wall," while keeping all critical functionality accessible to those with valid credentials. In today's democratized cyber environment, cost to attackers is substantially lower than cost to defenders. Thus it is useful to consider moving toward an architecture that is more akin to a building with all of its doors open, but riddled with traps and misdirection. As NC3 is modernized to utilize Internet-based protocols,[49] for instance, considering widespread implementation of mechanisms designed to increase costs to attackers via such methods as honeypots, script white-listing, and address scrambling would help to deter and frustrate potential attackers. Honeypots, or environments that look like useful targets to an attacker but are in fact benign, can be particularly useful in enabling U.S. personnel to identify candidate attack vectors and enact defenses before critical systems are compromised. Script white-listing entails using efficient data structures to enable a computer to run only code with a bit representation that has been explicitly pre-specified as part of an allowed execution set. Finally, address space scrambling methods such as address space layout randomization (ASLR) protect from common buffer overflow attacks by randomly arranging address space positions of key portions of a process, such that an attacker cannot jump between different points reliably.

As a higher-level consideration, the United States should consider the idea that it is generally not possible to be completely sure that a networked computer system has not been compromised. If an adversary informed the United States that it had compromised U.S. NC3 and that surety of the nuclear deterrent had been affected, it would be extraordinarily difficult for the United States to prove otherwise, which fundamentally undermines the strength of the U.S. deterrent posture. Thus, it is imperative that the United States be able to viably make the argument that compromising the entirety of NC3 would be a statistical impossibility; and for this to occur, there must exist no possible mechanism for a single point of failure. While the command, control, and communications triad architecture ensures this posture adequately from a physical standpoint, it is imperative that NC3 systems be constructed with the same ideas in mind. Specifically, the United States should consider a fractionated NC3 network design, with a large number of sub-networks, each secured via different sets of protocols or standards. In this case, it would be nearly impossible for an adversary to convince either itself, the United States, or third parties that the surety of the U.S. nuclear deterrent could be fully compromised by what would effectively be a first cyber strike.

Minimize Code Base Size

As systems are modernized to take advantage of twenty-first century information technology (IT), the temptation will exist to implement a great deal of additional functionality. While there may exist

48. "Turning Cyberattack Prevention into a SecOps Advantage," Cylance, 2015, https://www.cylance.com/hubfs/2015_cylance_website/assets/case_studys/Malware_SecOps_v3.pdf?t=1465600534915.

49. Fritz, "Hacking Nuclear Command and Control."

substantial operational benefits to additional features, these should always be balanced with the reality that more code almost always equates to more vulnerability—and NC3 is an area wherein a vulnerability could result in mistakes of nuclear import.[50] Thus, the usual analysis around the cost-benefit trade-off of IT upgrades may not apply to NC3 systems, and this reality should be taken into account in system design processes.

Maintain Small-Scale Launch and Inexpensive NC3 Communications Hardware

A particularly interesting suggestion put forth by Dr. John Harvey, former principal deputy assistant secretary of defense for nuclear, chemical, and biological defense, is that "small, single-purpose 'cheap-SATs' to replenish lost communication or GPS [global positioning system] functionality" could improve system-level resilience of space-based NC3 assets. Instead of or in addition to large, multifunctional satellites, leveraging the widespread proliferation of small, inexpensive CubeSats[51] that cost on the order of $100,000[52] to construct and launch could substantially reduce overall system cost and improve reliability. In addition to allowing inexpensive system updates as technology improves, these small satellites would be extremely difficult to target for ASAT operators. Further, since Dr. Harvey's address in 2014, small-scale launch technology has seen significant advances. In fact, several commercial entities currently have the technology to offer 150-kilogram payloads to sun-synchronous orbit (500-kilometer altitude) on a single dedicated rocket costing only $5 million.[53] These rockets could be retained specifically for emergency NC3 launches as backups to current satellites. In this way, expensive AEHF satellites that would require an expensive, large-scale launch to reconstitute would be supplemented or ultimately replaced by a small satellite and dedicated launch ecosystem that would result in a substantially more resilient NC3 system. Moving to a reserve of small satellites as a backup for the NC3 network would also have the advantage of increasing the number of possible launch sites the United States can use. At present, only a handful exist, and these are well-known to any potential adversary.[54]

Decrease Reliance on Space-Based NC3

In addition to shoring up the reliability of space-based NC3, ultimately decreasing U.S. reliance on these assets would likely enhance overall NC3 surety.[55] In particular, relying more on the various airborne components of the NC3 system and deploying "long-range airborne communications relay networks that could be stood up on short notice" would potentially mitigate the vulnerabilities posed by cyber threats to space-based assets. This risk reduction would result not only from the ability to more rapidly deploy space-based systems, but also from the simple reality that

50. Danzig, *Surviving on a Diet of Poisoned Fruit*.

51. A variety of companies (e.g., Planet Labs), universities, national labs (e.g., Los Alamos National Laboratory), and research institutions already fly multiple CubeSats.

52. "Commercial Space Launch Schedule and Pricing," Spaceflight.com, accessed 31 July 2016, http://www.spaceflight.com/schedule-pricing/.

53. "Space Is Now Open for Business," Rocket Lab, accessed 31 July 2016, https://www.rocketlabusa.com/.

54. Ellis, personal conversation with the author.

55. Rose, "Using Diplomacy to Advance the Long-Term Sustainability and Security of the Outer Space Environment."

performing diagnostics and updates on hardware that is not in outer space is a far simpler process than the reverse.[56]

Policy Considerations

Carefully Consider Unilateral Action: Anticipatory Self-Defense and Belligerent Reprisal

Given the *Tallinn Manual*'s clear authorization of anticipatory self-defense and the potentially dire consequences of the scenarios outlined above, it would be prudent to pursue a national policy that enables U.S. intervention to combat the development of cyber capabilities that would compromise NC3. In the context of peacetime international law, this would likely entail either claiming extraterritorial jurisdiction over those developing anti-NC3 cyber capabilities and/or claiming anticipatory self-defense if an attack is imminent. Were the United States to already be engaged in an armed conflict, the functional equivalent of anticipatory self-defense would be legally termed belligerent reprisal.[57] In this case, if the United States views attacks on NC3 as outside the boundaries established by the LOAC, the question would become whether a proportional attack on opponent (potentially on their NC3) would be appropriate, and, if so, what form that proportional response would take. Even in the case that U.S. NC3 is compromised, for instance, it is still desirable from the U.S. point of view for the adversary's NC3 systems to be able to verify that the United States has not launched a nuclear attack. Thus, in the context of belligerent reprisal, it is critical to make a clear policy decision on what constitutes a proportional, but practically optimal response to an attack on U.S. NC3.

Implement Cooperative Measures and Policy Standards

Perhaps most importantly, the United States should pursue implementation of cooperative measures to set international ground rules for interaction with NC3 systems. In an analogy to the military case, as recently as 2013 a Russian expert recommended developing a "non-binding international document prohibiting attacks on civil nuclear assets."[58] Further, the proposal suggests that the international community should improve existing cooperative instruments for "warning, interdiction, and consequence management" among nation-states. Separately, a similar conversation around norms and expectations for nation-state operation in space is already under way.[59]

Ultimately, U.S. security leaders have suggested that any technological progression that moves world powers, particularly the United States, Russia, and China, away from mutually assured destruction and toward the possibility of asymmetric first strike capability requires careful management. Richard Danzig, former secretary of the navy, suggests that if such a progression were to occur, the United States should directly engage Russia and China in pursuing multilateral

---

56. Harvey, "Nuclear Command and Control for the 21st Century."

57. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

58. EastWest Institute, *A Measure of Restraint in Cyberspace: Reducing Risk to Nuclear Civilian Assets* (New York: EastWest Institute, 2014), https://www.eastwest.ngo/sites/default/files/A%20Measure%20of%20Restraint%20in%20Cyberspace.pdf.

59. Rose, "Using Diplomacy to Advance the Long-Term Sustainability and Security of the Outer Space Environment."

agreements for parties to refrain from intrusion into nuclear warning, command, and control systems.[60] While this certainly represents a laudable goal, these agreements should perhaps move a step further and propose binding structures to combat any incursion into NC3 systems, enforcing them via some combination of sanctions and, if necessary, military force.

Separate NC3 and Conventional C3

Of all the policy recommendations considered here, the most direct and most effective would be to separate nuclear command and control systems from their conventional equivalents. While the current architecture may deter some low-level attacks by maintaining uncertainty about whether a particular cyber incursion would be considered nuclear in nature, it also comes with an inherent signaling risk that could lead to nuclear escalation. Were NC3 satellites to be explicitly separated from conventional C3 satellites and provided with a robust backup net (perhaps using a small satellite infrastructure), adversary intentions would be clarified substantially, and the United States could perhaps make its declaratory policy on NC3 incursions significantly more direct.

CONCLUSION

There remain many unanswered questions that both policymakers and operators need to consider as they move toward the next phase of NC3 technology. At present, assumptions are that NC3 is secured via a combination of air gaps, technological superiority in outer space and cyberspace, and human intervention in the control loop. Unfortunately, with the democratization of technology, asymmetric threats to space-based NC3 assets in particular have arisen that could fundamentally change the dynamics of nuclear strategic stability if not appropriately mitigated. To a degree, the uncertainty inherent in the current system can reinforce stability in the case of a risk-averse adversary, but could also undermine it in situations in which the adversary has nothing to lose.[61] A variety of technological initiatives including improving forensics, modernizing network defense, and moving to small satellite architectures could help improve the long-term surety of the NC3 architecture. Further, policy initiatives such as disaggregating nuclear and conventional C3, pursuing international agreements against NC3 incursions with key powers, and having a clear stance on application of the LOAC to cyber attacks on the nuclear enterprise would help both to mitigate risks to U.S. systems and actively deter malicious attacks against them. Ultimately, as the nation looks to maintain nuclear stability into the twenty-first century, it is imperative that critical nuclear security infrastructure be made robust to the myriad potential vulnerabilities resultant from the rapid spread of emerging technologies.

60. Danzig, *Surviving on a Diet of Poisoned Fruit*.

61. James Miller, personal conversation with the author.

U.S. Policy Toward Japanese Military Normalization

Dean Ensley[1]

This paper examines potential Japanese ballistic missile defense (BMD) policy options within their recent military normalization process. The purpose is to recommend the United States encourage specific policies explored by Japanese officials in order to improve U.S.-Japanese defense cooperation. Japanese efforts will have a significant effect on regional security dynamics and the U.S.-Japanese defense relationship. As such, it is beneficial for the United States to support those Japanese endeavors that offer the most potential for security in a dynamic region.

This analysis will also consider the parallel development of nuclear delivery systems from the Democratic People's Republic of Korea (DPRK) and the People's Republic of China (PRC) as the context that instigates Japanese-American ballistic missile defense improvements. Using data from a literature review and interviews with Japanese and U.S. defense officials, academic experts, and policymakers, this study evaluates options for BMD improvements. These potential improvements are assessed against metrics based on regional security risks, benefits to the U.S.-Japan alliance, and the feasibility of the programs.

Through this analysis, three recommendations are produced: outfitting existing Japanese destroyers with the Aegis Weapon System (AWS) platform, continuing U.S.-Japanese joint development of the SM-3 Block IIA missile, and opposing expansion of the Sea-Based X-Band Radar (SBX) program. Together, these policies would strengthen U.S.-Japanese BMD cooperation, counter rising regional threats, and avoid alarming other regional powers.

---

1. Dean Ensley is Implementation Manager at NES Associates in Alexandria, Virginia. Earlier, he interned at the Center for the Study of Weapons of Mass Destruction at the National Defense University. He holds a BSFS from Georgetown University and an MA from George Washington University.

INTRODUCTION

The Japanese post–World War II constitution of 1947 renounced the sovereign right of belligerency in war and the possession of war material.[2] As a result of the People's Republic of China (PRC) victory in 1949 and the DPRK invasion of the Republic of Korea (ROK) in 1950, the United States policy toward Japan shifted from that of an occupying power to that of a security patron, as it desired an economically vibrant Japan to act as a bulwark against communist encroachment in East Asia. Japan, benefiting from U.S. security guarantees and favorable access to U.S. consumer markets, rose within a few decades from the ruins of war to possess the world's second largest economy. However, in keeping with the intent of Article Nine of the Japanese Constitution, and a self-imposed limit to defense expenditure spending of 1 percent of gross national product since 1976, successive Japanese administrations historically did not develop a military force commensurate with the size of its economy.

This does not, however, suggest a lack of military investment over the years. As the Stockholm International Peace Research Institute (SIPRI) has recorded, Japanese military expenditures have built a powerful military even though capped at about 1 percent annually since 1988.[3] Under Prime Minister Shinzo Abe, Japan has pursued a policy of military normalization by seeking the conventional capabilities and political relationships associated with traditional national armed forces, in contrast to the historically limited scope of Japan's Self-Defense Forces (SDF). On July 1, 2014, the Abe administration announced its intention to reinterpret Article Nine to allow the SDF to participate in collective defense missions with other states. Due to a changing security environment in East Asia, the Abe government has correspondingly passed increasingly large defense budgets, including the record-sized ¥5.05 trillion (~$41.4 billion) in January, 2016.[4] Though this is still around the 1 percent benchmark, it represents an increase from the previous year's ¥4.98 trillion. The budget expands the SDF's conventional capabilities, funds new military technologies, and facilitates changes to the current doctrine and governmental defense structure. The Abe administration has also eased restrictions on arms exports, negotiated revision to the U.S.-Japan Defense Cooperation Guidelines, and sought to improve bilateral and multilateral relationships with other Asia-Pacific nations.

This paper will focus on the specific aspects of the process of Japanese military normalization relating to ballistic missile defenses. The United States should prioritize supporting Japanese endeavors in this area because they provide great potential for tangible cooperation and interoperability while directly countering the parallel threat of increasingly sophisticated delivery systems from the PRC and DPRK.

The purpose of this paper is to recommend U.S. policy responses to encourage specific BMD-related efforts undertaken by Japanese officials within the context of Japanese military

2. John Van Sant, Peter Mauch, and Yoneyuki Sugita, *Historical Dictionary of United States–Japan Relations* (Lanham, MD: Rowman & Littlefield, 2007), 114.

3. SIPRI, "Military Expenditure Database 2015," 2015, https://www.sipri.org/databases/milex.

4. Nobuhiro Kubo, "Japanese Defense Budget to Exceed 5 Trillion Yen in 2016/17," Reuters, December 23, 2015, http://www.reuters.com/article/us-japan-defence-budget-idUSKBN0U704N20151224.

normalization in order to improve U.S.-Japan defense cooperation and respond to regional threats. This is a significant area of research for two reasons. First, Japanese military normalization will have a notable effect on regional security dynamics and the Japanese-American defense relationship. Enhanced Japanese military capabilities will additionally affect other U.S. regional partners. Second, because Japan's military normalization efforts are relatively new and accelerating, a balanced debate regarding how the United States should respond is just beginning to develop in comparison to older, more established subjects.

A basic discussion of Japan's stance on the future of U.S.-Japan defense cooperation is necessary to understand the government's objectives. The Abe administration has three specific pillars to strengthen the U.S.-Japan security alliance: reinforcement of bilateral security and defense cooperation, cooperation based on strategic views of the Asia-Pacific region, and enhancement of cooperation in addressing global issues.[5] In the first pillar, Japan pursued negotiating revisions to the Japan-U.S. Defense Cooperation Guidelines in order to improve collaboration in maritime safety and security, BMD, cyber security, outer space, extended deterrence, and carrying out the realignment of the U.S. military forces in Japan. In the second pillar, Japan plans to work with the United States in enforcing the rule of law across the region, and promote partnerships and encourage trilateral cooperation with the ROK, Australia, India, and the Association of Southeast Asian Nations (ASEAN). This includes finalizing the Trans-Pacific Partnership and jointly addressing threats such as the DPRK tests and nuclear launches or the PRC's actions around the Senkaku Islands, known in the PRC as the Diaoyu Islands. In the third pillar, Japan plans to partner with the United States in addressing global challenges such as promoting women's empowerment, economic development, counterterrorism, climate change, and the conflicts in Ukraine, the Middle East, Africa, and elsewhere. Japan seeks to advance each of these three approaches to improving U.S.-Japan defense cooperation by carrying out numerous policy, doctrine, strategy, and technological modernizations.

This paper will first establish three key working assumptions. This paper will codify a series of metrics by which potential policy recommendations will be measured in order to establish their merit as an area the United States should endeavor to support as a method to improve U.S.-Japan defense cooperation. Additionally, this paper will compare existing BMD forces with developing regional delivery systems in order to identify existing strengths or weaknesses. This paper will focus on the most important delivery systems, due to length and scope limitations. Finally, this paper will present a series of policy recommendations for which BMD-related aspects of Japan's transformation the United States should support or resist in order to meet the regional threat.

KEY ASSUMPTIONS

In light of the prospective nature of this project and the potential for rapid change in relevant conditions, this paper operates under three key assumptions.

5. Interview A: official at Ministry of Foreign Affairs of Japan, March 12, 2015.

First and foremost, the Japanese government will continue to move toward military normalization. Japan's move toward a more robust security posture is a lengthy and ongoing process with roots in the early days of the Cold War. This process has been supported to varying degrees by multiple Japanese administrations, but the last decade has seen it move to the forefront of political discourse under Prime Minister Abe. Despite his first administration's internal scandals, Abe and the Liberal Democratic Party have enjoyed increased support for their efforts to expand the capabilities and range of actions available to the SDF. While continuing to face opposition from Komeito members within his ruling coalition, and other left-leaning political groups within Japan, Abe has addressed the threats posed by the PRC and DPRK with steadily increasing defense budgets and a cabinet-level reinterpretation of Article Nine. This paper assumes that this trend will continue as Japan pushes for a greater role, both regionally and internationally, even in the face of short-term economic difficulties or electoral setbacks for the Liberal Democratic Party.

Second, the United States will continue to support Japanese military normalization. The United States has already voiced its support for this process, as exemplified by high-profile visits to Japan by former secretary of defense Ashton Carter and President Barack Obama and the revision of the 1997 Guidelines for Japan-U.S. Defense Cooperation in 2015. U.S. diplomatic statements demonstrate a keen desire for a robust partnership with Japan that roots U.S. presence in East Asia.

Third, the PRC will continue to rise, and gray-zone scenarios will continue to plague the relationship between Japan and the PRC. Gray-zone scenarios, defined as "violations of Japanese sovereignty that are not military invasions requiring the issuance of a defense mobilization order but are beyond the policing capacity of the Japan Coast Guard,"[6] are not covered by a legal response mechanism or contingency plan and therefore pose a major risk of miscommunication or miscalculation. While the PRC will likely face significant economic and demographic challenges in the future, these are unlikely to limit its overall standing in the region in the near- to mid-term. Several flare-ups over disputed regional sovereignty, notably the question of the Senkaku-Diaoyu Islands, have brought the two nations closer to armed conflict. This paper assumes that no significant rapprochement will occur in the near- to mid-term that might substantially alter Japan's assessment of the strategic threat posed by the PRC.

METRICS OF VIABILITY

The potential policy options are measured against the following three metrics to provide a reasonable defense of their relative superiority.

1. Does it meet the threat to Japan's security?

    a. *It counters the regional threat.*

    This metric evaluates whether new political and strategic initiatives as well as specific intelligence and weapons platforms and programs promote a power balance that is in favor of the alliance, vis-à-vis the PRC and DPRK. By maintaining a favorable power balance, Japan

6. Tsuneo Watanabe, *Maritime Security and the Right of Self Defense in Peacetime: Proposals for a National Security Strategy and the New National Defense Program Guidelines* (Tokyo: Tokyo Foundation, 2014), 12.

will be able to maintain its territorial sovereignty and freedom of maneuver in the East Asia region and strengthen the U.S. regional position.

b. *It fills an SDF capability gap.*

This metric evaluates whether or not a military capability that the SDF did not previously possess has been developed. This could fill a niche capability, provide something that the United States cannot, or leverage a Japanese comparative advantage it possesses over its alliance partner due to its geographic proximity, economic integration, or cultural alignment in the region. This development will therefore have an outsized impact on the partnership's defense capabilities.

c. *It limits the regional security risks of military normalization.*

This metric evaluates programs and policies against their risk of provoking a more aggressive attitude or response from Japan's regional adversaries in the PRC and DPRK, causing a deterioration in ties between Japan and partner nations, such as the Republic of Korea or ASEAN members, or worsening the East Asian regional security environment in general. Promoting East Asian stability is a major goal of U.S. policy, and unresolved historical tensions and territorial conflicts between Japan and several of its neighboring states create vulnerabilities and sensitivities that must be carefully managed in Japan's process of military normalization.

2. Does it deepen U.S.-Japan defense integration?

a. *It contributes toward a joint posture.*

This metric evaluates the potential for a joint U.S.-Japanese posture. Such a posture can be described as military-military, political-political, civilian-civilian, or any combination of the three. Opportunities include humanitarian assistance and disaster relief, information, surveillance, and reconnaissance sharing, or maritime security. Increasing joint posture enables increasing awareness of interconnectedness, demonstrating collaboration to domestic audiences, and announcing collective efforts to the international community.

b. *It increases confidence within Japan for U.S. guarantees.*

This metric evaluates the clarity for Japanese domestic audiences regarding the U.S. commitment to the Asia-Pacific. As the United States is constantly involved in operations around the globe, the Japanese public is becoming increasingly skeptical of U.S. commitment to the region and needs reassurances. Moreover, there is worry about increasing U.S. public attention and realignment toward the PRC and away from Japan.

c. *It reduces the burden on the United States.*

This metric assesses the relative weight in security, economic, or political encumbrances carried by each nation. While each nation faces fiscal and domestic partisanship difficulties, the United States has numerous global responsibilities that limit its ability to dedicate resources to Japanese security. Burden reduction can come in the form of increasing Japanese military spending, political presence, or domestic willingness and support for military normalization.

3. Can it be implemented?

   a. *It is domestically palatable within Japan.*

   This metric assesses whether the policy would be acceptable to domestic audiences within Japan. While the Abe administration has been a major force behind military normalization, significant opposition still exists in the form of left-wing opposition parties, Abe's Komeito coalition partner, and a Japanese public that remains uneasy regarding military expansion.

   b. *It is domestically palatable within the United States.*

   This metric assesses whether the policy would be acceptable to domestic audiences within the United States. While the Obama administration is implementing the rebalance to the Asia-Pacific, the process of Japanese military normalization may or may not align with U.S. interests. There is at least broad support for this trend, but opposition could arise against specific Japanese policy changes or operational postures that may be undesirable for the United States.

   c. *It is within the current technological and industrial capabilities of involved parties.*

   This metric calculates feasibility in terms of the technology and industry requirements necessary for implementation. All involved parties must have the wherewithal and understanding in order to develop and produce new platforms, carry out new operations, and apply new policies. There must also be sufficient financial resources in order to accomplish the desired development.

THREAT ASSESSMENT

The government of Japan began preliminary consultations on BMD with the United States after the first Nodong flight test in 1993, leading to a U.S.-Japan joint study in 1995. Ultimately, following the 1998 Taepodong-1 flight test, Japan decided in 2003 to acquire BMD systems, and deployment of BMD units in the SDF finally began in 2007.[7] Current Japanese BMD forces include two primary interception systems: the land-based Patriot Advanced Capability-3 (PAC-3) and the sea-based AWS, which includes the AN/SPY-1 radar and either the Standard Missile-3 (SM-3) Block IA or Block IB.

Are PAC-3 missiles and the AWS sufficient to protect against regional delivery systems? And if not, what additional capabilities could help do so? Answers to these questions begin with a review of DPRK and PRC missiles.

As seen in Table 1, the DPRK maintains a robust collection of ballistic and cruise missiles. Of note are the Unha-3 and the developmental KN-08 and KN-11. The Unha-3 successfully launched a satellite into orbit in December 2012, which was a major accomplishment and fulfilled an ideological objective of the regime. Though not much information is available about it publicly, the KN-08 is road-mobile, based on a new transporter erector launcher, and was prominently displayed at

7. Fumio Ota, *The US-Japan Alliance in the 21st Century* (Kent, UK: Global Oriental, 2006), 117.

Table 1. North Korea's Ballistic and Cruise Missiles

Name	Other Names	Type	Payload (kg)	Range (km)	Status
KN-01	AG-1/HY-2	CM	N/A	150–200	Deployed
KN-02	SS-21	SRBM	250–500	120–160	Deployed
Hwasong-5	Scud B	SRBM	1000	300–320	Deployed
Hwasong-6	Scud C	SRBM	700	500	Deployed
Hwasong-7	Scud C	SRBM	400–750	700–1,000	Deployed
Nodong	Rodong	MRBM	250–700	1,300–1,500	Deployed
Musudan	Nodong-B	IRBM	1200	3,200–4,000	Development
Taepodong-1	Paektusan-1/Moksong-1	IRBM	100–200	2,500–5,500	Deployed
KN-08	Hwasong-13	ICBM	700	5,000–6,000	Development
Taepodong-2	Paektusan-2/Moksong-2/ Unha-2	ICBM/SLV	100–500	6,000–9,000	Deployed
Unha-3	Taepodong-3	ICBM/SLV	100–1,000	10000+	Deployed
KN-11	Pukgeukseong-1	SLBM	N/A	N/A	Development

Note: CM, cruise missile; ICBM, intercontinental ballistic missile; IRBM, intermediate-range ballistic missile; kg, kilogram; km, kilometer; MRBM, medium-range ballistic missile; N/A, not applicable; SLBM, submarine-launched ballistic missile; SLV, submarine-launched vehicle; SRBM, short-range ballistic missile.
Source: "Design Characteristics of North Korea's Ballistic and Cruise Missiles," Nuclear Threat Initiative, November 2014, http://www.nti.org/media/pdfs/design_characteristics_of_north_koreas_ballistic_and_cruise_missiles.pdf?_=1406744044.

military parades in 2012 and 2015. The KN-11's first test is believed to have been on January 23, 2015, and represents a nascent but potentially significant threat in the future.[8] DPRK delivery system development seems weighted toward intercontinental ballistic missiles (ICBMs) and submarine-launched ballistic missiles (SLBMs), marked by personal involvement of Kim Jong-un, widely released photographs, highly visible representation at military parades, and bellicose post-launch statements. One such statement, following the KN-11 launch, declared that "we now possess a world-class strategic weapon that can hit and eliminate enemy forces that attempt to

8. "Strategic Weapon Systems," *Jane's Sentinel Security Assessment: China and Northeast Asia* (February 2, 2016), 24.

harm our autonomy and dignity."[9] While bellicose statements are not uncommon, their consistency after widely proclaimed ICBM and SLBM launches are noteworthy.

China, too, has an increasingly diverse inventory of delivery systems, as shown in Table 2. Of note are the DF-21D, DF-41, and JL-2. The DF-21D represents an active effort to develop anti-access/area denial capabilities to control the Yellow, East China, and South China Seas. Official commentary of Beijing's September 3, 2015, military parade dubbed the DF-21D a "road-mobile anti-ship ballistic missile, the assassin's mace for maritime asymmetric warfare."[10] The core concept behind such weapons is that small, fast, expendable missiles are far less valuable than large, slower, expensive platforms such as aircraft carriers, and therefore inhibit a rival's willingness to deploy such large platforms to the theater. The DF-41, on the other hand, represents a Chinese desire to mirror U.S. and Russian multiple independently targetable reentry vehicle (MIRV)–capable ICBMs. A 2010 Pentagon report states that "the new generation of mobile missiles, maneuvering and MIRV warheads and penetration aids are intended to ensure the viability of China's strategic deterrent in the face of continued upgrades to U.S. and, to a lesser extent, Russian strategic intelligence, surveillance and reconnaissance; precision strike; and missile defense capabilities."[11] Though far more sophisticated, the DF-41 is similar to the DPRK's Unha-3 in terms of ideological and strategic role. Finally, the JL-2 fills a gap in China's strategic nuclear arsenal by providing a next-generation undersea deterrent for the new Jin-class or Type-094 strategic ballistic missile submarines (SSBNs).[12] This provides greater strategic flexibility, as demonstrated by the recent announcement that China will begin SSBN patrols in the wider Pacific Ocean.[13]

These developments suggest four strategic and ideological objectives (1) an ideological desire to be seen as on par with the top-tier missiles maintained by the United States and Russia in the DF-41 and Unha-3, (2) the development of an ocean-based nuclear deterrent in the KN-11 and JL-2, (3) an asymmetrical strike option in the DF-21D, and (4) a degree of resiliency in the road-mobile nature of the KN-08 and DF-41.

Are U.S. and Japanese PAC-3 missiles and the AWS sufficient to protect against such developments? Not in the long-term, arguably. The United States currently operates 16 Aegis-equipped surface combatants in the Pacific with the SM-3 Block IA or SM-3 Block IB missiles. The AWS is currently licensed to Japan in the form of four Aegis-equipped *Kongo*-class destroyers and Japan is in the process of upgrading two *Atago*-class destroyers with the AWS. There are currently 16 U.S. and Japanese PAC-3 units stationed in Japan. If these levels are maintained, rivals' increasing missile stockpiles and technological sophistication will eventually become dominant. In order to keep pace, the United States and Japan must increase the number of local

9. Ibid.

10. Andrew S. Erickson, "Raining Down: Assessing the Emergent ASBM Threat," *Jane's Navy International* (March 16, 2016), 3.

11. Robert Foster, "China Tests MIRV-Capable DF-41 ICBM," *Jane's Defence* Weekly (August 17, 2012), 2.

12. Nuclear Threat Initiative, "China," http://www.nti.org/learn/countries/china/delivery-systems/.

13. Julian Borger, "China to Send Nuclear-Armed Submarines into Pacific amid Tensions with US," *Guardian*, May 26, 2016, http://www.theguardian.com/world/2016/may/26/china-send-nuclear-armed-submarines-into-pacific-us.

Table 2. China's Ballistic and Cruise Missile Inventory

Name	Other Names	Type	Payload (kg)	Range (km)	Status
DF-3/3A	CSS-2	IRBM	2,150	2,800	Deployed
DF-4	CSS-3	ICBM	2,200	5,400	Deployed
DF-5/5A	CSS-4	MRBM/ ICBM	2,900/3,200 (MIRV)	1,200/13,000	Deployed
DF-21/21A	CSS-5 (Mod 1&2)	MRBM	600	2,150–2,500	Deployed
DF-21C	CSS-5 (Mod 3)	ASBM	600	1,750	Deployed
DF-21D	CSS-5 (Mod 5)	ASBM	600	1,550	Deployed
DF-15 (M-9)	CSS-6	SRBM	320–750	600	Deployed
DF-15A		SRBM	320–750	900	Deployed
DF-15B		SRBM	320–750	800	Deployed
DF-11 (M-11)	CSS-7	SRBM	800	280	Deployed
DF-11A		SRBM	500	350	Deployed
DF-31	CSS-10 (Mod 1)	ICBM	1,750	8,000	Deployed
DF-31A	CSS-10 (Mod 2)	ICBM	1,750	12,000	Deployed
DF-41		ICBM	2,500	12,000–15,000	Development
JL-1/1A	CSS-N-3	SLBM	600/500	2,150–2,500	Deployed
JL-2	CSS-N-5	SLBM	1,050–2,800	8,000	Deployed
HN-1		CM	N/A	650	Deployed
DH-10 (CJ-10)		CM	N/A	1,500–2,200	Development

Note: ASBM, anti-ship ballistic missile; CM, cruise missile; ICBM, intercontinental ballistic missile; IRBM, intermediate-range ballistic missile; kg, kilogram; km, kilometer; MIRV, multiple independently targetable reentry vehicle; MRBM, medium-range ballistic missile; N/A, not applicable; SLBM, submarine-launched ballistic missile; SRBM, short-range ballistic missile.
Source: "Design Characteristics of China's Ballistic Cruise Missiles," Nuclear Threat Initiative, November 2014, http://www.nti.org/media/pdfs/design_characteristics_of_chinas_ballistic_cruise_missiles_3.pdf?_=1421279197.

interceptors to reduce the threat of overwhelmingly local attacking missiles, and ensure BMD forces are flexible with regard to positioning to protect dispersed regional interests. Critical for the United States, any increased BMD forces should not appear offensive, thereby upsetting the status quo and triggering a disproportionate response from the PRC or the DPRK.

According to interviews with representatives in the Japanese Ministry of Defense (MoD), Japanese Ministry of Foreign Affairs, Takushoku University, and the Tokyo Foundation, Japan is seeking multiple avenues of improving its BMD capabilities. First, Japan is constructing new AWS destroyers, outfitting existing destroyers with the AWS, and considering seeking Aegis Ashore. Second, Japan contributes financial and technical resources to the SM-3 Block IIA development. Since 2012, Japan alone has spent ¥17.9 billion (~$168 million) on the Raytheon-Mitsubishi program.[14] The SM-3 Block IIA's 21-inch interceptor is larger than the 1A/B models' 14-inch interceptor, allowing for longer-range engagements and "a larger kill vehicle optimized for improved target detection and maneuverability."[15] The missile is to be deployed in the United States, Europe, and elsewhere within the next few years.[16] Interestingly, this intention to export the jointly developed system to third-party nations was a reason for the easing of Japan's Three Principles on Arms Exports, which was formalized on December 27, 2011.[17] Third, Japan is considering requesting permanent forward basing or increased production of the Sea-Based X-Band Radar (SBX).[18] The SBX-1, based in Adak Island, Alaska, and currently mothballed in Pearl Harbor, Hawaii, is a unique, self-propelled vessel and radar system without a concomitant interceptor.

POLICY ASSESSMENT

Policies and possible options for three weapons systems (AWS, SM-3 Block IIA, and SBX-1) are shown in Table 3.

Aegis Weapon System Policies

Does It Meet the Threat to Japan's Security?

- Destroyer-based Aegis and Aegis Ashore both counter the regional threat by providing additional tracking and interception capabilities.
- Though destroyer-related AWS options do not provide a new capability, destroyer-based Aegis provides a niche SDF projected mobile, BMD capability. All AWS choices, however, rely

14. Japanese Ministry of Defense, "Defense Programs and Budget of Japan, 2012–2016," http://www.mod.go.jp/e/d_budget/.

15. Amy Butler, "MDA Sees 2018 Deployment in Restructured SM-3," *Aviation Week*, August 7, 2012, http://aviationweek.com/awin/mda-still-sees-2018-deployment-restructured-sm-3-iia-plan.

16. Nuclear Threat Initiative, "Japan," http://www.nti.org/learn/countries/japan/delivery-systems/.

17. Ibid.

18. Interview A; Interview B: official at Takushoku University, March 9, 2015; Interview C: official at National Graduate Institute for Policy Studies, March 10, 2015; Interview D: official at Tokyo Foundation, March 10, 2015.

Table 3. Summary Matrix of the Policy Assessments for the Aegis Weapons System, Standard Missile-3 Block IIA, and Sea-Based X-Band Radar-1

Policy Assessment		Aegis Weapons System			Standard Missile-3 Block IIA	Sea-Based X-Band Radar-1	
		Construct Destroyers	Outfit Destroyers	Aegis Ashore	Joint Development	Increased Production	Forward Deployment
Secures Japan	Regional Threat	Y	Y	Y	Y	Y	Y
	SDF Gap	Y	Y	N	Y	Y	Y
	Regional Stability	N	Y	Y	Y	N	N
Integrates	Joint Posture	Y	Y	Y	Y	Y	Y
	U.S. Guarantee	Y	Y	Y	Y	Y	Y
	Burden Sharing	Y	Y	Y	Y	N	N
Feasible	Within Japan	Y	Y	N	Unsure	Y	Y
	Within U.S.	Y	Y	Y	Y	N	N
	Tech and lindustry	Unsure	Y	Y	Y	N	Unsure

Note: SDF, Self-Defense Forces.

on the AN/SPY-1 radar and the SM-3 missile so there is no technical comparative advantage.[19]

- Neither fixed Aegis Ashore positions nor upgrading additional destroyers with Aegis technology will antagonize regional adversaries. Conversely, constructing additional Aegis destroyers suggests a more aggressive maritime potential and will threaten the PRC's dominance of their coastal areas.[20]

19. Gilbert Rozman, ed., *Asia at the Tipping Point: Korea, the Rise of China, and the Impact of Leadership Transitions*, Joint U.S.-Korea Academic Studies, Vol. 23 (Washington, DC: Korea Economic Institute, 2012), 103, http://www.keia.org/sites/default/files/publications/tipping_point_full_book_final_version.pdf.

20. Interview B.

Does It Deepen U.S.-Japan Defense Integration?

- All three AWS options involve a U.S. technology, even if funded and operated by purely Japanese forces, and therefore contribute to a joint posture.
- As the AWS is an American technology, greater usage will promote positive views of the United States and therefore strengthen Japanese confidence in U.S. guarantees.
- None of the AWS options will reduce U.S. financial burdens, but they will allow the United States to realign BMD assets in the Asia-Pacific to support other strategic partners.

Can It Be Implemented?

- Aegis Ashore is not domestically palatable in Japan because people fear living in the vicinity of wartime targets and because it can be perceived as anchoring Japan to the defense of the United States, whereas destroyers are seen as a purely Japanese defensive mechanism. This fear of living near U.S. military installations is exacerbated by instances such as the murder on Okinawa.[21] Aegis destroyers, however, are regarded very highly within Japan.
- Licensing Aegis Ashore in Japan is likely domestically palatable for the United States as it is already being developed for allies, currently through the existing European Phased Adaptive Approach.[22]
- Additional Aegis destroyers or Aegis Ashore are feasible because the technology exists and the United States will likely continue licensing the technology to Japan as a major regional ally. However, the 2015 MoD budget's BMD allocation of ¥219.3 billion (~$2 billion) will likely not be sustained, which questions the continued viability of regularly constructing new destroyers.[23]

Joint Development of the SM-3 Block IIA

Does It Meet the Threat to Japan's Security?

- The SM-3 Block IIA meets the regional threat because its 21-inch diameter motor and kinetic warheads are specifically designed to provide improved velocity and range against short-, medium-, and intermediate-range ballistic missiles.
- It provides a new SDF capability of improved, sea-based interceptors.
- It is simply an improvement upon an existing platform and therefore has not, and likely will not, significantly antagonize regional rivals.

Does It Deepen U.S.-Japan Defense Integration?

- As a U.S.-Japan development, it symbolizes joint business and military partnerships.

21. Interview C.

22. Missile Defense Agency, "Aegis Ashore," fact sheet, July 28, 2016, https://www.mda.mil/global/documents/pdf/aegis_ashore.pdf.

23. Japanese Ministry of Defense, "Defense Programs and Budget of Japan, 2012–2016."

- It represents the U.S. role in Japanese BMD and therefore increases confidence in Japan for U.S. guarantees.
- It reduces the financial burden on the United States by outsourcing some design, production, and testing, as demonstrated by Japan's annual contribution of about ¥9 billion (~$90 million).

Can It Be Implemented?

- The SM-3 Block IIA is mostly acceptable in Japan, but some experts believe the Japanese role in producing a platform largely designed for European missile defenses signifies interconnectedness with European defenses, contrasting traditional Japanese security concerns being entrenched in the areas surrounding Japan (*shuhen*).[24]
- It is acceptable in the United States because it promotes the concept of distributed defense with Japan, as Raytheon is manufacturing the kill vehicle, Aerojet is building the first-stage motor, and Mitsubishi is building the nose cone, second-stage and third-stage motors, staging assembly, and steering control for the interceptor.[25]
- It is feasible because there is significant interest in both Japan and the U.S. defense and political communities for modernized interceptors, as well as sufficient funding and technological capability.

Sea-Based X-Band Radar Policies

Does It Meet the Threat to Japan's Security?

- The SBX-1 counters the regional threat by using 45,000 transmitter/receiver modules in an electronically scanned array to track baseball-sized objects at a distance of 2,500 miles in a full 360-degree azimuth and 90-degree elevation to provide mobile precision tracking, object discrimination, and missile kill assessment functions.[26]
- It provides a new, niche combination of features, though destroyers match its maritime mobility with even greater speed and Terminal High Altitude Air Defense also uses X-band radar.
- The current platform projects a purely defensive posture with increased sensory acuity and therefore does not currently provoke regional nations. Additional or permanent forward deployments, however, could.

Does It Deepen U.S.-Japan Defense Integration?

- The SBX-1 shares tracking data with Japanese forces and officials, and therefore contributes toward a joint posture.

---

24. Interview D.

25. Amy Butler, "Raytheon Eyes Early SM-3 IIA Builds," *Aviation Week*, March 13, 2014, http://aviationweek.com/defense/raytheon-eyes-early-sm-3-iia-builds.

26. Lawrence Kaplan, *A Brief History of the Sea-Based X-Band Radar-1* (Washington, DC: Missile Defense Agency, May 2008), 3, https://www.mda.mil/global/documents/pdf/sbx_booklet.pdf.

- It increases confidence in Japan for U.S. guarantees because it was specifically deployed in response to the April 2012 Unha-3 launch and redeployed after the similar December 2012 launch, exemplifying U.S. dedication to Japanese security.
- It does not reduce the burden on the United States because it is an entirely American endeavor, with American funding and implementation.

Can It Be Implemented?

- The SBX-1 is domestically palatable in Japan, even though its official mission prioritizes BMD protection for the "U.S. [and] its deployed forces," and it reinforces the idea that Japan is being anchored to the defense of U.S. assets.[27]
- Neither permanent forward basing plans nor the construction of additional SBX platforms are domestically palatable in the United States because it was a one-time project. Mike Arn, U.S. Army colonel and SBX project manager for the Missile Defense Agency (MDA), notes that it is "the only one of its kind" and "there are no current plans for another one."[28]
- It is technologically within the scope of U.S. production capability, but the construction yard has been disassembled and therefore no funding or industrial capability currently exists to produce more platforms. It is unclear whether funding could be secured for permanent forward basing.

POLICY RECOMMENDATIONS

Based on the above assessments, this paper recommends outfitting existing destroyers with the Aegis platform, continued development of the SM-3 Block IIA, and resisting any expansion of the SBX program.

Lease the Aegis Weapon System to Upgrade Japanese Destroyers

The U.S. Department of Defense (DoD) should continue to license the Aegis Weapon System to Japan in order to upgrade the BMD capability of additional destroyers, as has been done with the *Atago*-class. Potential platforms include the *Hatsuyuki*, *Asagiri*, *Abukuma*, and *Hatakaze* classes, all of which are funded for life extension measures in recent Japanese MoD budgets. In contrast to constructing new Aegis-equipped destroyers, upgrading existing platforms will counter the regional threat while not portraying an aggressive or expansive maritime posture. Destroyers provide the same BMD capabilities on a more flexible platform and are a prime example of the U.S. commitment to Japan. Moreover, using destroyers to provide a BMD function is more desirable than Aegis Ashore, which would force the United States to reconsider Aegis Ashore's current intended role as a European platform and be built in the vicinity of the Japanese public. If done on a ship-by-ship basis, continuing the current leasing design for Japanese platforms is advantageous for

27. Ibid.

28. "Followup: Sea-Based X-Band Radar (SBX) in Seattle, in Daylight," *West Seattle Blog*, May 11, 2011, http://westseattleblog.com/2011/05/followup-sea-based-x-band-radar-sbx-in-seattle-in-daylight/.

the United States because it will relieve American burdens to provide BMD and enables U.S. assets to be reallocated within the rebalance to the Asia-Pacific policy.

Continue Joint Development of the SM-3 Block IIA

The SM-3 Cooperative Development Program is the joint U.S.-Japan development of the SM-3 Block IIA. The SM-3 Block IIA represents an area ripe for cooperation. It provides a unique avenue for distributed defense, alleviates budgetary concerns for both nations, and improves the interceptor aspect of BMD. Despite being a potentially dual-use technology, the SM-3 platform is regarded as purely defensive and is not perceived as aggressive.

Resist Expanding the SBX Program

Japanese officials have expressed interest in a permanent forward basing plan or the construction of additional SBX platforms. The MDA should explicitly deny any possibility of additional production or permanent forward basing in Japan. Simply put, while the SBX-1 is a uniquely capable and useful platform, there is neither interest in the DoD nor operational necessity for further production. Additionally, its maritime mobility and radar functions are somewhat duplicated in other platforms, so its most significant contribution to the alliance is "showing the flag" through temporary deployments in response to crises. The MDA, and by extension the DoD, should reassert the SBX's role as a form of the U.S. guarantee for Japanese security, but resist any discussion of expanded operational uses, such as different mission priorities or deployments to the East or South China Seas. Based on this analysis, the further production of the SBX platform should not be pursued. Moreover, permanent forward deployment would lessen the symbolic value of occasional deployments in response to crises, and should therefore also not be pursued.

CONCLUSION

The successful implementation of the above policy recommendations would reliably meet the threat to Japan's security and significantly deepen U.S.-Japan defense integration. The recommendations do, however, face financial, institutional, and psychological barriers. The SM-3 Block IIA will incur continuing annual financial commitments for both nations encompassing research, development, testing, and system replacements. The U.S.-borne effort associated with enabling Japan to expand its Aegis-equipped destroyer fleet, in contrast, is mostly legal rather than financial, as the U.S. Congress must agree to license each platform individually. Resisting Japanese overtures for increased SBX platforms is a mostly psychological issue, as the system must continue to be portrayed as symbolic without suggesting its uniqueness negates the potential benefit of numerous platforms. As the May 2015 murder incident shows, there is still lingering concerns for both nations regarding permanent deployment of U.S. facilities on or near Japan, reinforcing the parallel recommendation to resist U.S.-manned deployment of Aegis Ashore to Japan.

Financial, legal, and psychological obstacles, though imposing, are surmountable. As demonstrated by Abe's speech to the U.S. Congress and the 2015 guidelines revision, there is abundant willingness to expand the nature and scope of the U.S.-Japan alliance. Abe hailed this partnership

as "an alliance of hope."[29] Japanese military normalization is advancing at an unprecedented pace and the United States should seek to promote its continuation as a form of supporting the rebalance to the Asia-Pacific and ensuring regional security and influence.

This is a significant topic because the Asia-Pacific is an increasingly dynamic region in which U.S. involvement must navigate economic and geopolitical complexities. Just as the European missile shield is postured against Iran but protects against Russia, so too will any U.S.-Japan BMD posture against the DPRK also protect against the PRC. The United States must therefore weigh individual expressions of support for Japanese security with the desire to prevent exacerbated tensions with the PRC. Consequently, all policy decisions must be implemented with dexterity.

Increased U.S.-Japan defense cooperation is not limited to the recommendations of this paper. The U.S.-Japan security alliance, a hallmark of the region for seven decades, continues to expand into new dimensions as political ties and technological cooperation have increased. This bodes well for the future of the U.S.-Japan alliance, but the United States must find the specific aspects of this expansion that offer the most potential for security in a dynamic region.

29. "Full text of Abe's speech before U.S. Congress," *Japan Times*, April 28, 2015, http://www.japantimes.co.jp/news/2015/04/30/national/politics-diplomacy/full-text-abes-speech-u-s-congress/#.VUZC7drBzGc.

Meeting Nuclear Policy Requirements with Modeling and Simulation

Ashley E. Green[1]

Modeling and simulation tools are key to understanding nuclear effects across the nuclear enterprise. From nuclear treaty monitoring to strategic planning, scientists and engineers use models to answer the questions of policy leaders and decisionmakers. As the community moves to build on legacy systems with modern computing technology, they must collaborate to create informative tools for end users beyond complex code development. Whether looking to understand employment of U.S. weapons or being prepared to detect a terrorist nuclear attack, the science is the same. Collaborating on development of nuclear effects tools is the only way to close technology gaps and ensure decisionmakers are informed in increasingly complex environments.

INTRODUCTION

Every aspect of the nuclear enterprise depends on modeling and simulation. Weapons designers model the super critical reaction of warheads. The treaty monitoring community simulates nuclear weapons effects to detect nuclear explosions across the globe. Military planners model the nuclear effects on targets to understand the many consequences of a nuclear strike. However, scientists and engineers are challenged by the lack of validation data from modern nuclear tests. Without the ability to test sensors and models against a live nuclear explosion, the forensics and

1. Captain Ashley E. Green is an active duty U.S. Air Force officer currently stationed at Air Force Research Laboratory, Kirtland Air Force Base (AFB), New Mexico, and is the program manager for the Nuclear Explosion Monitoring Program. Captain Green graduated from the U.S. Air Force Academy in 2011 with a bachelor of science in physics. Her first assignment was as a space systems analyst at the Air Force Technical Applications Center, Patrick AFB, Florida. In 2015, Captain Green received her master's degree in nuclear engineering from the Air Force Institute of Technology.

monitoring community and strategic planners rely heavily on modeling and simulation to understand the complex signatures generated by a nuclear detonation. Modeling and simulation have been integral to nuclear engineering since the development of the field in the early 1940s. From the use of analog computers to the implementation of IBM's punch-card style digital machines, computing power was vital to the progression of the nuclear enterprise.[2] Over 70 years later, today's nuclear engineers depend even more on computers to model all aspects of nuclear engineering.

After decades of tests at the Nevada Test Site, the United States has a wealth of knowledge of the effects of a nuclear detonation, as long as the detonation occurs on a clear day in the Nevada desert or Pacific atolls. Scientists and engineers have continued to study the effects of nuclear detonations using models but every variation from the baseline event leaves a question of simulation accuracy.

- How do wind, rain, or clouds change the growth of the fireball or movement of the plume?
- How do varied geological structures in the ground change the seismic signal?
- How will the shock waves interact with buildings in an urban area?
- How will fires spread in vegetation or infrastructure?
- How will buildings or other obstructions affect the ability to optically detect the flash of the fireball?

Even if nuclear testing was allowed, it would be impossible to perform the number and type of tests necessary to gather a comprehensive set of scientific evidence to account for the multitude of variations, including weather, terrain, and urban environments. Yet, understanding the broad effects of a nuclear detonation are necessary to answer two important policy questions. One, can the United States detect and respond to an adversaries' nuclear test or nuclear attack? Two, can the United States properly plan for employment of its own nuclear weapons and understand the full consequences of those actions?

In the past, nuclear monitoring was focused on detecting nuclear testing in controlled environments. Understanding the signal of an atmospheric detonation in an open test field with no visual obstruction is a much simpler problem than understanding the same detonation in, for example, the middle of Times Square. Finding the seismic signal of an explosion in a known test site is also easier than the resulting signal for a detonation in an underground parking garage. Even collecting samples of nuclear material becomes complex when the detonation is interacting with surrounding buildings. Similarly, there is a knowledge gap to understanding the complete effects of a nuclear strike on a given target and determining full consequence analysis. In order to improve the monitoring, forensics, and planning capabilities, engineers depend on modeling and simulation to answer these complex questions. The issue then, is how accurate are these models that cannot be validated against real data?

2. Atomic Heritage Foundation, "Computing and the Manhattan Project," accessed 31 May 2016, http://www.atomicheritage.org/history/computing-and-manhattan-project.

OVERVIEW OF NUCLEAR EFFECTS AND TECHNOLOGY

A nuclear detonation produces many dramatic effects on its surrounding environment. The large amount of energy released in a nuclear explosion creates a large shock front, radioactive fission products and gamma rays, a fireball hotter than the surface of the sun, an electromagnetic pulse (EMP), and earth tremors strong enough that seismometers created to detect earthquakes will register the event. All of these phenomena must be understood to plan for damage effects and for global monitoring and forensics.

The most distinct aspect of a nuclear explosion is the release of radioactive materials. The nuclear explosion is created by fissioning (i.e., splitting) atoms, primarily uranium-235 and plutonium-239. The fission process releases energy, gamma rays, a few neutrons, and fission fragments. These fission fragments are unstable, radioactive isotopes created by uranium and plutonium splitting apart. No other explosion will release these radioactive materials. Although longer-lived isotopes are also found in nature, a nuclear explosion will dramatically increase the ratio above the naturally occurring percentage. By monitoring air samples, the ratio can characterize an explosion as nuclear. Depending on the source of the uranium or plutonium used, the ratios of the radioactive materials might help to attribute the event to a particular region or source. The remaining, unburned uranium and/or plutonium and the resulting fission products released also cause radioactive fallout, a significant health and environmental concern for strategic planners that must be understood to predict collateral damage.

Nuclear detonations also create a shock front that causes ground tremors. Seismometers are used to detect the signals in the earth created by explosions. A nuclear or conventional explosion will create a signature different than an earthquake. Seismic signals propagate as body waves through the earth or as surface waves along the earth's surface. Body waves can also be separated into primary and secondary waves, known as P-wave and S-wave respectively. Earthquakes are distinguished by the larger presence of S-waves due to the shearing motion of an earthquake.[3] Distinguishing conventional from nuclear explosions is more difficult but may be accomplished in some cases by comparison with previous commercial explosion data.[4] Decades of research have improved the ability to characterize events through thorough data analysis and improving knowledge of the geologic variability in the earth for each region. For surface and low-altitude bursts, the shock front is also a primary damage mechanism of the detonation and the resulting effects are studied for the purpose of target planning.

Atmospheric detonations create many detectable signals including EMP and a fireball that can be detected as on optical flash. EMP is caused by the interaction of gamma rays with the surrounding air.[5] The gamma rays produce high energy free electrons via Compton scattering, the inelastic

3. National Research Council, *The Comprehensive Nuclear Test Ban Treaty: Technical Issues for the United States* (Washington, DC: National Academies Press, 2012), chapter 2.

4. Eli G. Baker, personal interview, May 1, 2016. Dr. Baker is a geophysicist for the Air Force Research Laboratory and works on the Nuclear Explosion Monitoring program.

5. Samuel Glasstone and Philip J. Dolan, eds., *The Effects of Nuclear Weapons*, 3rd ed. (Washington, DC: U.S. Department of Defense and Energy & Development Administration, 1977), http://www.deepspace.ucsb.edu/wp-content/uploads/2013/01/Effects-of-Nuclear-Weapons-1977-3rd-edition-complete.pdf.

collision of the gamma ray with electrons. The electrons interact with the earth's magnetic field to create an electric current that creates the electromagnetic field known as an electromagnetic pulse. The atmospheric detonation also creates a unique optical flash known to the monitoring community as the double-hump curve. The unique signal is created due to the visible surface temperature of the fireball created by the opaque outer shock front which absorbs the intense heat of the inner fireball. As the shock front cools it becomes more transparent and the more intense inner fireball begins to shine through in a phenomena known as breakaway, creating the second hump of the curve.[6] Understanding these effects is twofold, the phenomena can be used to monitor the globe for nuclear events but must also be analyzed to determine collateral damage of a nuclear strike.

ADVERSARIES ON ALLIES: NUCLEAR MONITORING AND FORENSICS

> *In a strange turn of history, the threat of global nuclear war has gone down, but the risk of a nuclear attack has gone up.*
>
> —President Barack Obama, Speech in Prague, Czech Republic, April 5, 2009

With the creation of nuclear weapons and the spread of its technology, the United States recognized the need to detect and monitor nuclear events. The United States developed its monitoring capability before any test limitation treaties existed and has continued to develop this technology for the purposes of treaty monitoring. Today, the United States has a network of sensors complemented by the International Monitoring System (IMS) utilized by the Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO).[7]

Further expanding on monitoring technologies, the United States recognized the need for nuclear forensics in the case of domestic nuclear attack. Forensics is used to determine the type of weapon and its origin. In 2006, the National Technical Nuclear Forensics Center was established within the Department of Homeland Security as part of the Domestic Nuclear Detection Office.[8] The National Technical Nuclear Forensics Center is tasked to enhance the nation's nuclear forensics capabilities in order to quickly respond to an attack.[9] Quickly and accurately determining who is responsible allows the United States to prosecute those responsible.[10] Having the capability to attribute the nuclear detonation can act as a deterrent, as those responsible can be held accountable for their actions. In complex urban environments, the expected location of an attack, forensics capabilities rely on modeling and simulation technology to test new sensor systems.

---

6. Ibid., section 2.122.
7. National Research Council, *The Comprehensive Nuclear Test Ban Treaty*, chapter 2.
8. U.S. Department of Homeland Security, "National Technical Nuclear Forensics Center," accessed 20 March 2016, https://www.dhs.gov/national-technical-nuclear-forensics-center.
9. Ibid.
10. Ibid.

The Air Force Technical Application Center (AFTAC), the Department of Defense (DoD) nuclear treaty monitoring and nuclear event detection agency, depends on modeling and simulation not only for event analysis and forensics but for training purposes as well.[11] Currently AFTAC has two methods of creating simulations for training satellite alert officers on event detection. The first is SIMTOOL, an in-house program that has the ability to quickly be integrated into the mission system for training purposes.[12] The second method is working with Sandia National Laboratory for more robust simulations, although this is limited due to the time and availability of personnel.[13] Sandia's simulations can take months to generate and deliver to AFTAC for use. AFTAC has begun leveraging other advanced models produced by the national laboratories and industry, and has begun investing in high-performance computing (HPC) resources.[14] While these steps will help improve the modeling capability both for training and mission assurance, a process for collaboration among the nuclear community is necessary to continue to close technology gaps.[15] Bringing in innovative industry techniques can speed development beyond in-house research methods.

RESPONDING TO A TERRORIST NUCLEAR ATTACK IN A CITY

Although the threat of global nuclear war has diminished, the threat of a terrorist nuclear attack in a city has increased.[16] The forensics community has started to modify legacy models and sensors in order to respond to a nuclear explosion in a city. The technical improvement must be made in order to answer two questions. First, it is necessary to determine if an explosion is nuclear as quickly as possible in order to properly respond to the emergency situation. Second, the forensics capability to ascertain the type of weapon used is crucial in determining the perpetrators. A key initiative in U.S. nuclear policy is to hold accountable any state or non-state actor that enables terrorists to obtain or use weapons of mass destruction.[17]

The more complex the environment of the detonation, the more difficult it becomes to understand the data collected and determine the nature of the weapon. Nuclear testing sites produce more predictable results of the effects than in a complex urban environment. The challenge is to modify tools developed to analyze a simple scenario and build upon them to analyze data from a more complex event. Improving tools will require bringing in industry resources that technically complement current methods. The United States has begun to find the answers to the complexities with the establishment of the National Technical Nuclear Forensics Center

11. Patrick Wingate, personal interview, June 13, 2016. Mr. Wingate is the lead for training and evaluation of the satellite alert officers at AFTAC.

12. Ibid.

13. Ibid.

14. Ibid.

15. Ibid.

16. U.S. Department of Defense (DoD), *Nuclear Posture Review Report: April 2010* (Washington, DC: DoD, 2010), https://www.defense.gov/Portals/1/features/defenseReviews/NPR/2010_Nuclear_Posture_Review_Report.pdf.

17. Ibid.

but scientists are still limited by technology that cannot be tested and validated against an actual nuclear detonation.

ALLIES ON ADVERSARIES: OVERVIEW OF STRATEGIC PLANNING

The effects that allow monitoring and detection of a nuclear explosion are the same effects that cause damage to enemy targets in the event of a U.S. nuclear strike. The shock front creates the blast. Thermal radiation vaporizes, melts, or combusts materials depending on the relative location to the source. Radioactive fission fragments cause radiation poisoning to people and the environment. EMP damages electronics. Current tools may limit the ability of the United States Strategic Command (USSTRATCOM) to inform the president of broader consequences of nuclear strike options, efficiently plan for employment of nuclear forces, and evaluate operations risks of proposed options.[18] Conventional explosives have predictable effects but nuclear explosions can result in extensive collateral damage beyond the initial blast, depending on interactions with the surrounding environment.

In determining strike options, planners must understand how the United States employs its nuclear weapons. The Air Force Nuclear Weapons Center (AFNWC) is charged with sustaining the Air Forces nuclear capabilities. Part of those capabilities is ensuring that U.S. weapons can be effectively employed; this includes determining flight profiles for nuclear bombers to have safe escape routes after dropping a nuclear bomb, providing mission characteristics for the Department of Energy to sustain nuclear components of the weapon, and ensuring the weapon is protected in all environments until it is deployed for use.[19] From ensuring an intercontinental ballistic missile (ICBM) is not damaged in flight to updating nonnuclear components for sustainment of weapons in storage, every step in the process of sustaining U.S. nuclear capabilities depends on modeling and simulation. Planners must understand limitations of weapons employment to determine strike options. The AFNWC works to model mission profiles to ensure effective employment to meet strategic nuclear planners requirements.

PLANNING FOR COLLATERAL DAMAGE IN NUCLEAR TARGETING

Collateral damage of nuclear effects must be examined to give the full political, military, and socioeconomic implications of U.S. action.[20] Strategic nuclear planners depend on scientists and engineers to calculate collateral damage possibilities of a nuclear strike option in order to inform

18. "Course of Action Decision Brief for Adm Cecil D. Haney, USSTRATCOM Commander," briefed by Dr. Michael Kuliasha, director for nuclear technologies, Defense Threat Reduction Agency, June 15, 2015.

19. Col. Edward Jakes, personal interview, June 30, 2016. Colonel Jakes is the chief scientist at the AFNWC.

20. Ibid.

internal planning processes and produce materials for presidential decision support.[21] Similar to monitoring capabilities, planning for collateral damage must account for complex changes in the environment. Models need to account for various target types, from an isolated underground bunker to a military building near an urban area.[22] In addition to target location, planners also require tools that can deliver quick real-time results as well as tools for long-term planning that may provide more fidelity, allowing for more detailed analyses.[23]

Recognizing the limitations of current modeling and simulation capabilities, the Defense Threat Reduction Agency (DTRA) has been charged with filling the technology gaps in order to improve presidential decision support and develop consequence analysis tools to help nontechnical strategic planners understand the extended effects of a nuclear strike.[24] The Collaborative Nuclear Targeting Analyses (CNTA) program was initiated by DTRA in 2015 to address some of USSTRACOMs strategic nuclear planning questions.[25] CNTA is looking to extend models beyond traditional damage mechanisms and account for secondary, collateral damage caused by effects such as fire, radiation, or EMP.[26] In order to complete these tasks, CNTA leverages the power of high-performance computing and the collaboration of U.S. nuclear experts across the nuclear enterprise to develop and modernize tools.[27] DTRA's programmatic strategy relies on this broad collaborative approach to reduce development time and ensure a breadth of U.S. subject matter experts are contributing to the development. The key is to develop incremental capabilities, first focusing on collateral damage, before increasing fidelity of the models.[28]

In development of the new tools for planning and consequence analysis, it is important to consider the needs of the end user beyond the technical results. DTRA is working to understand the needs of USSTRATCOM early in the process in order to produce results that are meaningful to planners who do not have a doctorate in nuclear engineering. This process involved creation of regions of concern based on time, type of damage, and location of damage. Consequence analysis capabilities must support analyses ranging from deliberate planning, which takes place on the order of weeks, to time-sensitive planning with much shorter timelines.[29] Analyses must account for damage to the target and damage in the target area as well as the broad political, military, social, and economic consequences to damage beyond the target, for example, whether

21. "Memorandum for the Director, Research and Development, Defense Threat Reduction Agency," signed by Maj. Gen. David D. Thompson, director for plans and policy, USSTRATCOM, October 17, 2014.

22. "CNTA Target Scenarios," briefed by Steve Shafer, Sandia National Laboratory, May 2016.

23. "2015 Defense Nuclear Users Group Table Top Exercise Outbrief," Defense Threat Reduction Agency (DTRA), October 19–23, 2015.

24. Matthew Kurtz, personal interview, July 6, 2016. Mr. Kurtz works in the Office of the Secretary of Defense for Nuclear Planning Policy.

25. Jeffrey McAninch, personal interview, May 25, 2016, and June 9, 2016. Dr. McAninch is the project manager for CNTA.

26. "CNTA Target Scenarios," briefed by Steve Shafer, Sandia National Laboratory, May 2016.

27. "Course of Action Decision Brief for Adm Cecil D. Haney USSTRATCOM Commander," briefed by Dr. Michael Kuliasha.

28. Ibid.

29. McAninch, personal interview, May 25, 2016, and June 9, 2016.

fire will spread beyond the target or whether EMP produces power outages throughout the city. These effects could greatly increase the number of unintended casualties beyond the intended target. Models must produce casualty estimates that account for the prompt and delayed effects of a nuclear detonation in order to provide decisionmakers with the knowledge to examine the feasibility and acceptability of nuclear strike options.[30] Meeting the diverse needs will not be easy and will require effective collaboration between scientists and engineers across the enterprise and industry. No piece of the puzzle is trivial and scientists face the same limitations as those working in the forensics community: there is very little data to use in validating and verifying models.

IMPROVING MODELING AND SIMULATION TOOLS FOR POLICY LEADERS AND DECISIONMAKERS

Although limitations to validation remain, both the forensics and strategic planning communities have enhanced the process of improving models and simulations. To further improve models and close technology gaps it is important that programs focus on collaboration between organizations and look for innovative ideas outside of the nuclear enterprise. Many agencies are looking to solve the same nuclear effects questions, and collaboration is the only way to find answers with the limited available resources. Computing power and technology increase exponentially, and it is important to utilize new technology to continually improve nuclear effects models. Scientists and engineers often become comfortable with a specific computer code or method but, by increasing collaboration outside the nuclear enterprise and utilizing fresh ideas, the nuclear scientific and engineering community may be able to increase the speed at which it develops tools to answer policy leader questions.

Along with collaboration, engineers must always keep in mind the end user of their work. Technical experts can get lost in the scientific aspects of their work without acknowledging the goal. The focus of the models and simulations should be on how the results will be used by policymakers and strategic nuclear planners as they begin to understand the highly technical nature of nuclear planning.[31] Producing a tool with the most cutting edge technical means is not useful if the decisionmakers cannot understand and accept the results. The Defense Nuclear Users Group (DNUG) noted the importance of including training on the tools.[32] Every step of the way, the scientists and engineers must recognize the end users and collaborate with them throughout development. Policymakers are not looking for a quantitative answer but results that can bound the most reasonable scenario.[33] Decisionmakers planning for use of a nuclear weapon want a probable answer with high confidence that gives the number of fatalities and not the extensive analysis used to determine the answer.[34] Creating tools to answer technology

30. Ibid.
31. "2015 Defense Nuclear Users Group Table Top Exercise Outbrief," DTRA.
32. Ibid.
33. Kurtz, personal interview, July 6, 2016.
34. Ibid.

gaps is only useful if the engineers can use those tools to generate relevant products for decisionmakers.[35]

By utilizing advanced computing technology, the United States can bridge the technology gap. Collaboration and end user focus are key to success. In recent years, the forensics and strategic planning communities took the first step forward by recognizing the importance of the problem. Moving forward, program managers must ensure that scientists and engineers remain innovative in closing the technology gap. The national security environment is always changing and U.S. nuclear experts must work to remain ahead.

CONCLUSION

Whether the task is to monitor the globe for nuclear explosion, determine the damage of a strike scenario, or use forensics to characterize a nuclear explosion, the key to success is through models and simulations. Although there is historic test data, there is not a comprehensive data set across the many complex scenarios to fully validate models. Across the nuclear enterprise, agencies are beginning to realize the need to close technology gaps and start collaborative efforts to quickly develop new tools in order to answer policy questions. Modeling one nuclear effect in a scenario is a complex problem, and combining all nuclear effects makes the problem exponentially more difficult.

Besides developing new modeling tools, it is also necessary to consider the end users of the product. Whether it is a satellite alert trainee, strategic planner, or policy decisionmaker, the tools are only as useful as the final product is comprehensible to the end users. Throughout the development of future tools the end users should be part of the discussion. Experts across the nuclear enterprise should also consider reviving nuclear effects education to build relationships between the technical and policy experts.[36]

From monitoring and forensics to strategic planning, every organization is looking to utilize modern computational techniques to create better models of nuclear effects and scenarios. Each organization is beginning to close technology gaps to answer leadership questions. As these organizations move forward, it is necessary that they form a collaborative effort because no matter what complex nuclear scenario they are looking to answer, the basis is the same understanding of nuclear effects. In order to prepare policymakers for a real-world event, collaboration between the nuclear enterprise organizations and willingness to include new technologies from outside industry are necessary to shorten the timeline. No matter the changes in the national security environment, it will always be necessary to have modeling and simulation tools available to keep leaders informed on nuclear technologies and policy impacts.

35. "2015 Defense Nuclear Users Group Table Top Exercise Outbrief," DTRA.

36. Ibid.

Assessing the Nuclear Lessons of the First Gulf War

Rebecca Friedman Lissner[1]

How did the conventional military dominance that the United States demonstrated during the First Gulf War shape its post–Cold War nuclear policy? In analyzing the nuclear lessons of the Gulf War, this paper investigates how conventional warfare shapes states' nuclear postures and strategies more generally. Nuclear-armed states frequently conduct conventional military operations. Yet, in emphasizing the categorical difference between nuclear and conventional weapons, existing scholarship largely overlooks the influence of conventional warfare on nuclear strategy. Based on examination of primary and secondary sources, as well as interviews with participants, I find three types of nuclear lessons learned from the Gulf War. First, the most important nuclear lessons were the danger posed by regional powers' nuclear proliferation, and the United States' insufficient tools to counter this proliferation. Second, the Gulf War convinced policymakers that precise conventional systems could increasingly substitute for nuclear systems, though changes in nuclear strategy reflect the end of the Cold War as well as the lessons of Desert Storm. Finally, there is incomplete evidence that the Gulf War changed the United States' approach to conflict escalation. Cumulatively, these findings substantiate my conclusion that conventional warfare can change the way states view the utility and efficacy of their nuclear arsenals, as evidenced by modification of states' nuclear posture and strategy.

The First Gulf War broke out at a moment of acute strategic uncertainty for the United States. With the Cold War clearly coming to a close, the grand strategy of containment was no longer an apt organizing principle for U.S. foreign policy. Similarly, the nuclear force posture that supported containment's aims was no longer necessary to preserve U.S. security in a post–Cold War world. Iraq's invasion of Kuwait prompted the first major crisis of the "new world order" and provoked U.S. military intervention. Although the ultimate political success of the Gulf War remains contested,[2]

---

1. Rebecca Friedman Lissner, PhD, is a Stanton Nuclear Security Fellow at the Council on Foreign Relations.

2. Stephen Biddle, "Victory Misunderstood," *International Security* 21, no. 2 (October 1, 1996): 139; Joshua Rovner, "Delusion of Defeat: The United States and Iraq, 1990–1998," *Journal of Strategic Studies* 37, no. 4 (2014): 482–507.

its military success was staggering. U.S. conventional warfighting abilities—largely untested in combat since Vietnam—demonstrated the potential of the information revolution, as precision-guided munitions enabled pinpoint strikes against regime targets and global positioning system (GPS)–guided troops maneuvered in the desert with unprecedented coordination.[3] How did the conventional dominance that the U.S. military demonstrated during the Gulf War shape its post–Cold War nuclear policy?

In analyzing the nuclear lessons of the Gulf War, this paper investigates how conventional warfare shapes states' nuclear postures and strategies more generally. Nuclear-armed states frequently conduct conventional military operations. In emphasizing the categorical difference between nuclear and conventional weapons, however, existing scholarship largely overlooks the influence of conventional warfare on nuclear strategy.[4] Because a nuclear war has never been fought, it is impossible for policymakers to directly assess the validity of their nuclear-strategic calculations; instead, they look to conventional uses of force for information. Consequently, this paper evaluates the proposition that lessons learned from conventional warfare shape the nuclear dimensions of grand strategy in two significant and underappreciated ways: first, by demonstrating the intentions and resolve of adversaries, and, second, by influencing policymakers' assessments of crisis escalation dynamics as well as the relative utility of nuclear and conventional systems.

Studying the Gulf War illuminates important connections between conventional war and nuclear strategy. Primary and secondary sources suggest that George H. W. Bush's administration learned important nuclear lessons from the Gulf War. The Gulf War demonstrated that Washington had overestimated the Iraqi threat—and, by extension, that of the Soviet Union and its client states—and underestimated the United States' own military capabilities. This paper seeks to examine the nuclear implications of these strategic miscalculations. How did the Gulf War change the way U.S. policymakers thought about the role of nuclear weapons in a post–Cold War world, specifically: (1) the nature of nuclear threats in the 1990s and beyond, (2) the relative utility of nuclear versus conventional systems for deterrence and war fighting, and (3) escalation dynamics in likely post–Cold War contingencies?

Based on examination of primary and secondary sources, as well as interviews with participants, I find that the danger posed by undetected nuclear proliferation, and the United States' insufficient tools to counter this proliferation, emerged as the most important nuclear lessons of the Gulf War. The Gulf War also convinced policymakers that precise conventional systems could increasingly substitute for nuclear systems, though changes in nuclear strategy reflect the end of the Cold War as well as the lessons of Desert Storm. Finally, I find weak support for the proposition that the Gulf War changed the United States' approach to conflict escalation. Cumulatively, these findings substantiate my conclusion that conventional warfare can change the way states view nuclear weapons, including states' nuclear posture and strategy.

---

3. Michael Gordon and Bernard Trainor, *The Generals' War: The Inside Story of the Conflict in the Gulf* (Boston, MA: Little, Brown, 1995), xii.

4. See, for example, Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989).

NUCLEAR THREATS IN THE 1990S AND BEYOND

The most decisive lesson that the Bush administration took from the Gulf War was the danger posed by aggressive regional powers armed with nuclear weapons. The war highlighted the danger of such rogue nuclear states because, during Desert Storm and afterward, inspectors found that the Iraqi nuclear program was substantially more advanced than U.S. intelligence previously indicated. Although proliferation was a concern prior to the Gulf War, "disclosure of Iraq's clandestine nuclear weapons program and its use of ballistic missiles during the Gulf War accelerated the expansion of nuclear doctrine."[5]

The U.S. intelligence community's underestimate of the progress of Iraq's nuclear weapons program came as a shock, highlighting the risks of undetected nuclear proliferation. The post-war Gulf War Air Power Survey stated these conclusions starkly:

> The Iraqi nuclear program was massive, for most practical purposes fiscally unconstrained, closer to fielding a nuclear weapon, and less vulnerable to destruction by precision bombing than Coalition air commanders and planners or U.S. intelligence specialists realized before Desert Storm. The target list on 16 January 1991 contained two nuclear targets, but after the war, inspectors operating under the United Nations Special Commission eventually uncovered more than twenty sites involved in the Iraqi nuclear weapons program; sixteen of the sites were described as "main facilities."[6]

The miscalculation was all the more alarming to policymakers because of the specific method Iraq used to create fissile material.[7] The Iraqi facilities employed electromagnetic isotope separation to enrich uranium, a process that required vast quantities of electricity to power.[8] Bush administration officials were confounded—and alarmed—that U.S. intelligence had not picked up on such intensive energy usage.

Moreover, after-action reports revealed that the U.S.-led bombing campaign had failed to substantially degrade the Iraqi nuclear program as well as Saddam Hussein's arsenal of Scud missiles. Even the much-lauded precision systems, famously capable of penetrating individual building windows in Baghdad, made few inroads on key weapons of mass destruction (WMD) targets. To quote the Gulf War Air Power Survey's findings:

---

5. Kristensen and Handler add, "The war had just ended when Secretary Cheney issued the post–Gulf War top secret Nuclear Weapons Employment Policy (NUWEP) which formally tasked the military to plan for nuclear operations against nations capable of or developing weapons of mass destruction." Hans M. Kristensen and Joshua Handler, *Changing Targets: Nuclear Doctrine from the Cold War to the Third World* (Amsterdam: Greenpeace International, 1995), 4.

6. Eliot A. Cohen, *Gulf War Air Power Survey*, vol. 1 (Washington, DC: Office of the Secretary of the Air Force, 1993), 78, http://books.google.com/books?id=pYNtAAAAMAAJ.

7. Author interview with George H. W. Bush administration Department of Defense (DoD) official, April 2015.

8. Federation of American Scientists, "Iraqi Nuclear Weapons," May 2012, http://fas.org/nuke/guide/iraq/nuke/program.htm.

> The Iraqi nuclear program's redundancy, advanced status on the eve of the war, and elusiveness, in conjunction with the extraordinary measures the Iraqis took immediately after Desert Storm to conceal its extent by destroying certain facilities, led the United Nations to conclude that the air campaign no more than "inconvenienced" Iraqi plans to field atomic weapons.[9]

Difficulties in destroying Iraqi Scuds and chemical weapons caches further undermined policymakers' confidence that rogue states' nuclear weapons programs could be degraded militarily—even with new, high-end systems.[10]

As a result of these revelations, counterproliferation rose to the top of the Bush administration's strategic objectives. Nolan wrote, "In the aftershock of Operation Desert Storm, the redefinition of proliferation from a diplomatic priority to an urgent military priority became a central preoccupation of policymakers."[11] Nuclear proliferation was the most extreme concern because nuclear weapons would provide aggressor states with the capability to counter superior U.S. forces asymmetrically, threatening emergent U.S. hegemony as well as myriad regional interests.[12]

Such conclusions extended beyond the Bush White House to Democrats who later staffed the Clinton administration at the highest levels. For example, Representative Les Aspin—who was then the chairman of the House Armed Services Committee but would go on to serve as President Bill Clinton's first secretary of defense—offered Saddam Hussein's Iraq as the template for future "threat driver[s]."[13] Indeed, other pariah states with potential WMD programs were measured against Iraq as a "threat yardstick" to determine the extent of their aggressiveness, as well as the military resources necessary to counter them.[14] By the mid-1990s, "'countering' the acquisition and use of weapons of mass destruction by regional proliferators . . . [became] a central focus of [U.S.] nuclear strategy."[15]

Lessons from Iraq also galvanized interest in bolstering the nonproliferation regime. Beginning in 1993, the International Atomic Energy Agency (IAEA) initiated an effort to supplement the Nuclear Non-Proliferation Treaty (NPT) with extra safeguards against secret nuclear programs.[16] Although Iraq had been a party to the NPT, it exploited a loophole in the NPT that limited inspections and monitoring of declared facilities. The Additional Protocol, formalized in 1997, sought to identify

---

9. Cohen, *Gulf War Air Power Survey*, 82.

10. Ibid., 81, 83, 89.

11. Janne E. Nolan, *An Elusive Consensus: Nuclear Weapons and American Security after the Cold War* (Washington, DC: Brookings Institution Press, 2001), 68.

12. See, for example, *National Security Strategy of the United States: 1991* (Washington, DC: White House, August 1991), 31.

13. Les Aspin, *An Approach to Sizing American Conventional Forces for the Post-Soviet Era: Four Illustrative Options* (Washington, DC: Government Printing Office, 1992).

14. Ibid. See also Nolan, *An Elusive Consensus*, 68.

15. Kristensen and Handler, *Changing Targets*, 3.

16. "The 1997 IAEA Additional Protocol at a Glance," Arms Control Association, April 2015, https://www.armscontrol.org/factsheets/IAEAProtoco.

and deter construction of secret nuclear sites ("undeclared facilities") by giving the IAEA inspectors broader inspection authority.[17]

RELATIVE UTILITY OF NUCLEAR AND CONVENTIONAL SYSTEMS

The United States' conventional preponderance in the Gulf War convinced U.S. strategists that high-tech conventional weapons could increasingly substitute for nuclear weapons in underwriting the security of the United States and its allies. U.S. military performance in the Gulf War substantiated the administration's view that, in the words of Secretary of State James Baker, "precision guidance enables the conventional weapons of today to destroy targets that in years past were assigned primarily to nuclear weapons."[18] Moreover, the Gulf War experience suggested that conventional weapons could successfully deter adversaries armed with unconventional weapons, like Iraq's chemical and biological arsenal.[19] Indeed, shortly after the war, the Bush administration announced its willingness to forswear the U.S. chemical arsenal.[20]

The precise role played by nuclear threats in deterring Iraqi chemical weapons use during the Gulf War remains contested. Many contemporaneous sources laud the apparent success of nuclear threats in deterring Iraq from employing missile-launched chemical weapons, indicating that nuclear weapons remained useful against regional adversaries.[21] After the war, some analysts highlighted the deterrent effect of President Bush's eleventh-hour letter to Saddam, delivered to Tariq Aziz, Iraq's foreign minister, by Secretary of State James Baker in Geneva, which affirmed Washington's willingness to employ "all means available" in retaliation for Iraqi chemical weapons

---

17. Arshad Mohammed, "Iraq, North Korea Failures Shadow Nuclear Talks with Iran," Reuters, July 1, 2015, http://www.reuters.com/article/2015/07/01/us-iran-nuclear-verification-idUSKCN0PB5HY20150701.

18. Excerpt of Baker confirmation hearing: "Transition in Washington: Excerpts from Baker's Testimony before Senate Committee," *New York Times*, January 18, 1989, http://www.nytimes.com/1989/01/18/us/transition-in-washington-excerpts-from-baker-s-testimony-before-senate-committee.html?src=pm&pagewanted=1. McGeorge Bundy wrote in October 1991,

> Especially in the pinpoint accuracy of the most advanced systems, conventional weapons displayed a capacity for discrimination that no system dependent on nuclear explosions could ever hope to reach—not only because of the side effects of even low-yield nuclear weapons, but still more because of the enormous psychological shock of any nuclear attack.

McGeorge Bundy, "Nuclear Weapons and the Gulf," *Foreign Affairs* 70, no. 4 (October 1, 1991): 83–94.

19. Bobby Inman et al., "U.S. Strategy after the Storm," in *After the Storm: Lessons from the Gulf War*, ed. J. S. Nye and R. K. Smith (Lanham, MD: Madison Books, 1992), 241, 261.

20. Ibid., 280.

21. For example, William Arkin, "US Nukes in the Gulf," *Nation*, December 31, 1990, 834; Robert Toth, "American Support Grows for Use of Nuclear Arms," *Los Angeles Times*, February 3, 1991; David Broder, "US Forces Have No Nuclear Arms in Gulf States, No Plans to Use Them," *Los Angeles Times*, October 2, 1990; Ed Gilley, "N-Threat Deterred Saddam," *Seattle Post-Intelligencer*, May 17, 1991.

use.[22] Yet others have questioned the role of U.S. nuclear threats in deterring Iraqi unconventional weapons. One former policymaker recalls that the administration's expectation was that Saddam would use chemical weapons only if his regime survival depended on it; thus the president's decision to leave Saddam in power was more determinative than his nuclear threats.[23] Moreover, intelligence assessments publicized after the war indicate that Iraq may have been technically incapable of fielding Scud-delivered chemical warheads.[24]

Ultimately, regardless of their actual deterrent value, "assessments of the coalition victory against Iraq helped legitimate the importance of nuclear threats in deterring Saddam Hussein from launching chemical and perhaps biological weapons against Western forces and allies."[25] In the context of policy debates at the time, these conclusions undermined advocates for a no-first-use policy.[26]

Moreover, U.S. policymakers continued to see a role for nuclear weapons in the post–Cold War world—a role substantially informed by their perceived utility against future Iraq-like regional contingencies.[27] According to Arkin, the Gulf War bolstered the credibility and utility of nuclear threats in the eyes of the Pentagon, contributing to a "post–Gulf war doctrine that assigns expanded roles to nuclear forces, specifically to deter the use of WMD, including chemical and biological weapons."[28] Indeed, nuclear weapons were perceived as useful against the proliferation threats highlighted by Iraq's nuclear weapons program. The commander of Strategic Command (STRATCOM), General Lee Butler, advocated for a conception of nuclear deterrence that encompassed nuclear proliferation.[29] Butler's was not an isolated view; in 1992, Secretary of Defense Richard Cheney issued a Nuclear Weapons Employment Policy, which "formalized procedures for nuclear operations against countries with the potential to develop weapons of mass destruction."[30] The strategy of maintaining nuclear capabilities as a hedge against future contingencies endured through the Clinton administration's major nuclear policy statements, specifically the 1993 Bottom-Up Review,[31] 1994 Nuclear Posture Review (NPR), and Presidential Decision

22. For additional instances of implied nuclear threats made by the Bush administration and directed at Iraq, see William M Arkin, "Calculated Ambiguity: Nuclear Weapons and the Gulf War," *Washington Quarterly* 19, no. 4 (1996): 5.

23. Author interview with former George H. W. Bush policymaker, April 2015. This claim is possibly belied by a February 24 Situation Report from Central Command (CENTCOM), cited in Arkin, which stated: "We expect Iraq to initiate chemical operations within 24 hours" of the ground war's commencement. Arkin, "Calculated Ambiguity," 7.

24. Nolan, *An Elusive Consensus*, 74–75.

25. Ibid.

26. Andy Butfoy, "Washington's Apparent Readiness to Start Nuclear War," *Survival* 50, no. 5 (2008): 115–140.

27. Kristensen and Handler, *Changing Targets*. For a perspective that emphasizes disarmament trends in the early 1990s, see Josiane Gabel, "The Role of U.S. Nuclear Weapons after September 11," *Washington Quarterly* 28, no. 1 (Winter 2004/2005): 181–195.

28. Arkin, "Calculated Ambiguity," 4. As an example, Arkin cites Joint Chiefs of Staff, *Doctrine for Joint Nuclear Operations*, Joint Publication Nos. 3–12, December 18, 1995.

29. Nolan, *An Elusive Consensus*, 67.

30. Ibid., 64–65.

31. Kristensen and Handler, *Changing Targets*, 6–7.

Directive 60 in 1997.[32] Similarly, the George W. Bush administration's 2002 NPR emphasized threats from "terrorists or rogue states armed with weapons of mass destruction"[33] and the Obama administration's 2010 NPR, which made "preventing nuclear proliferation and nuclear terrorism" its top objective.[34]

To address the anticipated threats of the 1990s, in the wake of the Gulf War, U.S. nuclear posture and strategy adapted to and integrated with new conventional systems for maximal efficacy. The creation of STRATCOM cemented the convergence of nuclear and conventional missions.[35] As the nuclear mission refocused away from the Soviet Union and toward regional threats, STRATCOM assumed responsibility for rapid and flexible targeting—a major change from the single integrated operational plan (SIOP) that had characterized nuclear targeting during the Cold War. According to Nolan:

> As General Lee Butler, commander of STRATCOM, saw it, the design of small nuclear options that could be retargeted quickly as the need arose would bring nuclear weapons into closer conformity with conventional forces and make their potential utility on the battlefield more credible. The restructuring of [Strategic Air Command, known as] SAC into STRATCOM transferred responsibility for planning regional nuclear options from the regional commanders to STRATCOM, allowing it to take over target planning for strategic and nonstrategic forces against states with weapons of mass destruction. Using adaptive planning and the reserve force, STRATCOM could implement a variety of attack options against regional threats in a matter of hours.[36]

An approach emphasizing nuclear flexibility in response to regional contingencies persisted into the Clinton administration and beyond. The 2002 NPR, for example, introduced the concept of a "new triad," one leg of which constituted "offensive strike systems (both nuclear and nonnuclear)."[37]

The greater integration of nuclear and conventional war planning, combined with the fall of the Soviet Union, precipitated important changes to U.S. nuclear posture. While the end of the Cold

---

32. Gabel, "The Role of U.S. Nuclear Weapons after September 11," 185. Additionally, Arkin writes that during 1993 discussions about the Nuclear Posture Review, "there was a strong [belief] . . . underscored by the Gulf 'experience,' that the threat to use nuclear weapons could deter undesirable enemy actions, and that nothing should be done to undermine that deterrent effect." Arkin, "Calculated Ambiguity," 13.

33. "Nuclear Posture Review [Excerpts]" January 8, 2002, http://web.stanford.edu/class/polisci211z/2.6/NPR2001leaked.pdf.

34. U.S. Department of Defense, *Nuclear Posture Review Report: April 2010* (Washington, DC: DoD, April 2010), http://www.washingtonpost.com/wp-srv/politics/documents/2010NuclearPostureReviewReport.pdf?sid=ST2010040601668.

35. Gregory Gilmour, "From SAC to STRATCOM: The Origins of Unified Command over Nuclear Forces" (master's thesis, Naval Postgraduate School, June 1993), 58–59, http://www.dtic.mil/dtic/tr/fulltext/u2/a268609.pdf.

36. Nolan, *An Elusive Consensus*, 65.

37. "Nuclear Posture Review [Excerpts]," January 8, 2002.

War likely had the greatest role in inspiring Bush's Presidential Nuclear Initiative,[38] it seems plausible that the Gulf War shaped the administration's confidence in the determination that tactical nuclear weapons were no longer necessary to defend South Korea,[39] and the decision to cease "normal" deployment of tactical nuclear weapons on surface ships, attack submarines, and naval aircraft.[40] Ultimately, nuclear weapons remained important to U.S. national defense, but their significance lessened with the end of the Cold War and the performance of advanced conventional systems in the Gulf War; as a result, defense procurement priorities swung decisively toward conventional systems.[41]

ESCALATION DYNAMICS

While the greater substitutability of conventional and nuclear weapons had implications for conflict escalation dynamics, the precise effect is difficult to capture empirically. Because the United States spent most of the past 25 years fighting unconventional wars against non-state actors, the necessity of climbing the escalatory ladder remained blessedly remote. Nevertheless, primary and secondary sources suggest a few ways in which the Gulf War may have shaped U.S. strategists and planners' thinking about wartime escalation dynamics.

First, the fact that the Gulf War never escalated beyond conventional forces signaled that nonuse norms would persist in the post–Cold War world.[42] President Bush explicitly rejected nuclear use in December 1990, prior to commencement of the air campaign against Iraq. The timing of this decision is significant because the president expected a tough fight against Saddam's million-man army, but nevertheless ruled out nuclear use. The military was apparently unaware of the president's decision; while war plans that included nuclear weapons were proposed, they were not seriously considered.[43]

Second, the demonstrated efficacy of conventional weapons may have pushed nuclear options farther up the escalatory ladder. For example, Bill Perry, who later became secretary of defense, wrote in 1992 that the conventional capabilities demonstrated in the Gulf raised the nuclear threshold for the first time since the 1950s; advanced-technology weapons might prove more effective deterrents, he argued, because unlike nuclear weapons these conventional systems were

38. Susan Koch, *The Presidential Nuclear Initiatives of 1991–1992*, Case Study 5 (Washington, DC: National Defense University Press, September 1992), http://ndupress.ndu.edu/Portals/68/Documents/casestudies/CSWMD_CaseStudy-5.pdf.

39. This shift on tactical nuclear weapons was reflected in the Bush administration's arms control position. Paul Wolfowitz, "Shaping the Future: Planning at the Pentagon, 19891993," in *In Uncertain Times: American Foreign Policy after the Berlin Wall and 9/11*, ed. M. P. Leffler and J. W. Legro (Ithaca, NY: Cornell University Press, 2011), 55.

40. Interview with Clinton administration official, November 2014. On the Presidential Nuclear Initiative's changes to nuclear force posture, see Hans Kristensen, "The Neither Confirm Nor Deny Policy: Nuclear Diplomacy at Work," Nuclear Information Project, February 2006, http://www.nukestrat.com/pubs/NCND.pdf.

41. Bundy, "Nuclear Weapons and the Gulf."

42. Ibid., 83–94.

43. Arkin, "Calculated Ambiguity," 3.

highly usable.[44] The result was that "the United States would no longer need to extend its nuclear forces to deter nonnuclear attack" on allies—a conclusion that never became declaratory policy but nevertheless shows the important nuclear lessons drawn by influential elites from conventional warfare in the Gulf.

Yet, a third, contradictory lesson may also have emerged about the utility of nuclear weapons in certain contingencies. Advances in conventional technologies created the possibility of smaller-scale nuclear strikes, possibly making nuclear weapons more usable. To some extent, this change reflects diminished fears of mutually assured destruction given that most-likely contingencies entailed regional powers with little or no nuclear arsenals. Yet, coupled with advances in low-yield nuclear weapons technology, the precision revolution augured by the Gulf War may have lowered the threshold for nuclear use over the long term by diminishing the anticipated destruction of a nuclear detonation. Indeed, Kristensen and Handler contend that proliferation anxiety after the Gulf War inspired the U.S. military to pursue new, low-yield miniature and "exotic" nuclear options.[45]

IMPLICATIONS FOR POLICY AND SCHOLARSHIP

The preceding discussions demonstrate that U.S. policymakers did learn nuclear lessons from conventional warfare in the Gulf War of 1990–1991. Specifically, policymakers took the following lessons:

- Nuclear proliferation by regional powers can be difficult to detect and poses a threat to vital U.S. national interests. Counterproliferation is thus a top national security priority.
- High-tech conventional systems, such as those demonstrated in the Gulf War, can increasingly substitute for nuclear systems, but a role remains for nuclear weapons in deterring and countering WMD use and proliferation.
- Given existing technology, new conventional systems raise the threshold for nuclear use, but precision-strike technology holds the potential for introducing low-yield nuclear weapons that might ultimately lower the threshold for nuclear use.

To conclude I ask whether, in light of the past 25 years of international politics, these lessons have proven correct.

Nuclear Threats

In the realm of nuclear threats, covert nuclear proliferation by regional powers remains a primary national security concern. Given the United States' global interests, as well as its continued conventional military superiority, nuclear weapons are an attractive asymmetric tool for states

44. Inman et al., "U.S. Strategy after the Storm," 241.

45. Kristensen and Handler quote George Miller, Lawrence Livermore associate director, drawing direct connections between the Gulf War's "revelation" of Iraq nuclear capability as well as its demonstration of precision delivery, which together suggest the possibility of low-yield nuclear weapons directed at counterproliferation targets. Kristensen and Handler, *Changing Targets*, 13–14.

threatened by U.S. power. Yet the nuclear-alarmist predictions of the 1990s have not been realized, and nuclear proliferation has posed less of a threat to American interests than many imagined.[46]

Indeed, alarmism led to some significant foreign policy blunders. In contemplating the 2003 invasion of Iraq, George W. Bush administration policymakers—many of whom had also served during the first Gulf War—extrapolated from previous experience and assumed that the Iraqi nuclear program was farther along than intelligence indicated. Yet the 2003 Iraq War demonstrated that Saddam Hussein had an incentive to strategically misrepresent the progress of the Iraqi nuclear program because of domestic-political imperatives as well as regional power dynamics—even though this misrepresentation ultimately provoked war with the United States.[47]

More broadly, the nonproliferation regime seems to have advanced U.S. interests in countering the spread of WMD more effectively than U.S. nuclear saber rattling. At the same time as the military was developing new operational concepts for countering WMD, U.S. diplomats led Nuclear Non-Proliferation Treaty (NPT) signatory states in extending the NPT indefinitely at the 1995 review conference. In addition to its normative value in affirming the nuclear taboo—a taboo that would be undermined by American use of nuclear weapons to counter nuclear proliferation—the NPT provides a framework for deterring prospective proliferators through cost-imposing strategies.[48] Recent academic research finds that sanctions, like those imposed on states in violation of their NPT obligations, are remarkably effective in deterring nuclear proliferation.[49]

Relative Utility of Nuclear and Conventional Systems

In spotlighting the threat of nuclear proliferation, the Gulf War provided support to those who argued that nuclear weapons would remain a necessary component of the U.S. defense posture in the post–Cold War world. At the same time, the war's demonstration of advanced conventional capabilities augured a new era of warfare in which the nuclear threshold could be substantially higher.

The command performance of new military technologies in the Gulf War prompted widespread triumphalism, only somewhat tempered by postwar revelations that the air war had not been as effective as originally thought. Strategy documents written after the Gulf War highlight U.S. technological superiority as an advantage that the United States must maintain. Some argue, however, that the United States did not go far enough in pursuing advantages offered by the military-technical revolution enabled by the information age. Analysts associated with the Defense Department's Office of Net Assessment argue that "most observers had lost interest in the revolution in

46. Francis J. Gavin, "Same as It Ever Was: Nuclear Alarmism, Proliferation, and the Cold War," *International Security* 34, no. 3 (January 1, 2010): 9–13.

47. David A. Lake, "Two Cheers for Bargaining Theory: Assessing Rationalist Explanations of the Iraq War," *International Security* 35, no. 3 (2010/2011): 29–30.

48. On the nuclear taboo, see Nina Tannenwald, "Stigmatizing the Bomb: Origins of the Nuclear Taboo," *International Security* 29, no. 4 (2005): 5–49.

49. Nicholas L. Miller, "The Secret Success of Nonproliferation Sanctions," *International Organization* 68, no. 4 (2014): 913–944.

military affairs by 2002 or 2003," most likely because the counterinsurgency wars in Afghanistan and Iraq demanded different materiel. As a result, the promise of the precision-strike regime did not fully "mature."[50]

Initially, the shock and awe of the Gulf War seems to have convinced potential competitors that the United States' technological advantage was unbridgeable. The Russian military was reportedly quite impressed with U.S. capabilities, and the Gulf War made a similarly strong impression on the Chinese.[51] Yet, rather than deterring competition, this realization elevated the importance of nuclear weapons for conventionally weak states. After the Gulf War, India's chief of army staff famously summarized the lesson of the war for the rest of the world: "Don't fight the Americans without nuclear weapons."[52] Indeed, in 2008 an analyst observed "a commonly expressed U.S. view inside and outside the Bush administration that overwhelming U.S. conventional capabilities have provided a stronger driver for nuclear proliferation than nuclear weapons."[53] The example of U.S.-sponsored regime change in Iraq in 2003 made this imperative all the more acute for states deemed "rogue" by the U.S. government. For those states that cannot afford a conventional hedge against U.S. military power, nuclear weapons appear the best asymmetric options; states that can afford to compete conventionally, like China, have pursued precision-strike capabilities alongside nuclear modernization.

In addressing the increased salience of nuclear weapons, the United States has performed fairly well. As mentioned above, nonproliferation has succeeded to a greater extent than many thought possible in the early 1990s. Yet the U.S. national security establishment has only begun to grapple with the prospect of reentering a world in which wartime nuclear detonations are plausible. Despite the greater salience of nuclear weapons, the United States was correct in pursuing the revolution in military affairs to the extent that it did; these capabilities, together with nonproliferation efforts, meaningfully advanced U.S. goals in stopping the spread of nuclear weapons to new states.

Over the past five to ten years, however, the renewed specter of great-power rivalry has introduced a troubling category of challenges. Alongside diplomatic strategies, competing with prospective challengers like Russia and China requires that the United States continue to maintain its conventional edge, perhaps by pursuing the precision-strike regime to full maturity. Additionally, the need to enhance deterrence may militate in favor of the continuation of nuclear modernization policies pursued by the Obama administration, such as delivery systems like the long-range

---

50. Author interview with DoD official in the Office of Net Assessment, April 2015; Barry D. Watts, *The Maturing Revolution in Military Affairs* (Washington, DC: Center for Strategic and Budgetary Assessments, 2011), http://csbaonline.org/uploads/documents/2011.06.02-Maturing-Revolution-In-Military-Affairs1.pdf.

51. See, for example, T. Gongora and H. Von Riekhoff, *Toward a Revolution in Military Affairs?: Defense and Security at the Dawn of the Twenty-First Century*, Contributions in Military Studies (Westport, CT: Greenwood Press, 2000), 97; D. L. Shambaugh, *Modernizing China's Military: Progress, Problems, and Prospects* (Berkeley: University of California Press, 2002).

52. Christopher F. Chyba, "'Time for a Systematic Analysis: US Nuclear Weapons and Nuclear Proliferation," *Arms Control Today* 38, no. 10 (2008): 24–29.

53. Ibid.

standoff (LRSO) nuclear-armed cruise missile, and refurbished weapons like the recently tested B61-12, which reportedly provides greater accuracy and variable yield.[54]

Escalation Dynamics

Over the past 25 years, strategic thought about nuclear escalation has more closely reflected the lessons of normative constraint and elevated nuclear thresholds. Overall, the United States has seen its interests aligned with advancing the nuclear taboo—though Washington's commitment to the taboo has never been tested in a major crisis—and the NPT. For reasons described above, this lesson seems to have been a valid one. For normative as well as strategic reasons, the nuclear threshold remains very high. U.S. military planners do not seem to have identified missions with solely nuclear paths to success. Increasingly, conventional options can fulfill nuclear missions, a prospect illustrated by ongoing debates over conventional prompt global strike.

While these same advances in precision strike might have been leveraged for nuclear systems, the low-yield options that some anticipated in the wake of the Gulf War have been slow to materialize. Between 1994 and 2004, Congress banned research and development on nuclear weapons of fewer than five kilotons in the Spratt-Furse precision low-yield weapon design (PLYWD) provision to the fiscal year (FY) 1994 National Defense Authorization Act. Though Congress repealed this provision in 2004, advocates of expanding low-yield options contend that the U.S. military remains ill-equipped in that domain.[55] Despite its 2010 NPR commitment not to build new nuclear weapons, the Obama administration has worked to enhance the flexibility of existing nuclear weapons. As mentioned above, modifications included in the B61-12 Life Extension Program seem to finally fulfill the post–Gulf War prediction that precision guidance would ultimately be married with lower-yield bombs. The B61-12 has an internal guidance system for targeting, as well as four yields—0.3, 5, 10, and 50 kilotons—according to media reports.[56] While the nuclear threshold ought to remain very high, changes in the geopolitical environment substantiate the deterrent value of maintaining a range of nuclear options for the president.

As Thomas Schelling elucidated, nuclear politics are strategic: they necessarily entail dynamic interactions between two or more players.[57] Assessing the nuclear lessons that the United States learned from the Gulf War is thus incomplete without a parallel assessment of the lessons learned by current and prospective competitors. American strategists were correct when they recognized that the United States emerged from the Cold War as the world's sole superpower, militarily

---

54. On the LRSO nuclear-armed cruise missile, see Marina Malenic, "USAF Wants to Dodge Latest Air Defences with Bomber's New Secret Weapon," *IHS Jane's Defence Weekly*, January 27, 2015. On the B61-12, see Mike Hoffman, "Nuclear Bomb Upgrade Could Violate Key Treaty," *Defensetech*, February 28, 2014; Marina Malenic, "US Completes First B61-12 LEP Flight Test," *IHS Jane's Defence Weekly*, July 18, 2015.

55. Keir A. Lieber and Daryl G. Press, "The Nukes We Need," *Foreign Affairs*, November 1, 2009, http://www.foreignaffairs.com/articles/65481/keir-a-lieber-and-daryl-g-press/the-nukes-we-need; Kier A. Lieber and Daryl G. Press, *Coercive Nuclear Campaigns in the 21st Century: Understanding Adversary Incentives and Options for Nuclear Escalation* (Monterey, CA: Naval Postgraduate School, 2013), https://www.hsdl.org/?view&did=734062.

56. Mike Hoffman, "Nuclear Bomb Upgrade Could Violate Key Treaty," *Defensetech*, February 28, 2014.

57. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1980); Thomas C. Schelling, *Arms and Influence: With a New Preface and Afterword* (New Haven, CT: Yale University Press, 2008).

unrivaled and diplomatically dominant. But far from implying a holiday from history, this exceptional position requires great effort and shrewd strategy to maintain. With the reemergence of great power politics in Asia and Europe, it is time for policymakers to revisit the lessons of the Gulf War and to assess whether prevailing assumptions about nuclear policy remain appropriate to the present international security environment.

Russian Pre-Nuclear Deterrence: Nonnuclear Options for Strategic Effect

Harrison Menke[1]

As an effort to manage conflict at higher levels of escalation, Russian strategists have begun to analyze how to leverage advanced conventional tools to impose costs and de-escalate hostilities without crossing the nuclear threshold. Termed pre-nuclear deterrence, this strategy relies on the threat of escalation to radically transform the nature of a conflict and compel an opponent to manage hostilities. Looking to convey resolve and risk in the hopes of sustaining advantage—or avoiding defeat—in an escalating conflict, Russia may well see nonnuclear options that have the potential to achieve strategic results as a more tolerable escalation option than recourse to the limited use of nuclear weapons. This paper will review pre-nuclear deterrence and how it may be operationalized using a framework derived from Russian military journals and influential writings, and offer modest North Atlantic Treaty Organization (NATO) force posture proposals to deal with this emerging challenge.

INTRODUCTION

Using nonnuclear means to impose costs and help manage escalation is a subject of growing interest among Russian strategic thinkers. In 2014, Russia's new military doctrine (a modified version of the 2010 doctrine) established nonnuclear deterrence as a strategic goal.[2] However,

---

1. Harrison Menke is a research analyst at the National Defense University's Center for the Study of Weapons of Mass Destruction. His work focuses on nuclear forces, deterrence, and regional conflict and escalation. The author would like to thank his colleagues at the center for their helpful comments. The views expressed are the author's and do not necessarily reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. government.

2. "Military Doctrine of the Russian Federation," December 2014, http://www.mid.ru/documents/10180/822714/41d527556bec8deb3530.pdf/d899528d-4f07-4145-b565-1f9ac290906c.

little more has followed to explain how contemporary Russian strategists think about nonnuclear deterrence: What problems does it purport to solve? How would it be operationalized? How does it contribute to a Russian theory of victory for regional conflict?[3]

With some notable exceptions, these important questions have yet to be fully assessed by Western experts.[4] This paper seeks to add to current research by examining Russian concepts and theories on pre-nuclear deterrence. This paper first explores former Russian first deputy minister of defense and leading strategic thinker Andrei Kokoshin's pre-nuclear deterrence model and how it may be operationalized using a framework derived from Russian military journals and influential writings. Subsequent sections address evidence of pre-nuclear deterrence thinking in Russia's Syria operations and critically assess the Russian "theory of victory." The paper concludes by conceptualizing a NATO offset and offers some modest force posture proposals. This paper is not intended as a definitive guide to Russian pre-nuclear doctrine. Rather, it showcases aspects of Russian thinking on the subject in order to better understand how the Kremlin might utilize pre-nuclear deterrence in a time of acute crisis.

PRE-NUCLEAR DETERRENCE FOUNDATIONS

Over the last decade, Andrei Kokoshin has attempted to work through aspects of the nonnuclear deterrence challenge, and his most significant contribution focuses on approaches for managing conflict at higher levels of escalation. Termed pre-nuclear deterrence, Kokoshin's strategy is designed to deter a high-end adversary by bridging the gap between a rapidly escalating conventional conflict and the limited use of nuclear weapons. Pre-nuclear deterrence is intended to provide options short of nuclear use to counter a form of conventional aggression that relies on air dominance and the use of precision munitions.[5] Integrated precision-strike campaigns, like those used by the United States in Iraq and Yugoslavia, are considered the principal threat to Russian security, due in large part to Russian conventional military weaknesses.[6] As a consequence, Russia has heavily relied on nuclear weapons to deter or repel such strikes. Kokoshin and other Russian analysts assert that complete reliance on nuclear deterrence is no longer satisfactory (if it ever was), as the threat of nuclear use may only be credible at the highest levels of conflict.[7]

---

3. For additional insight into theories of victory, see Brad Roberts, *The Case for Nuclear Weapons in the 21st Century* (Stanford, CA: Stanford University Press, 2016).

4. Experts include Brad Roberts, James Bosbotinis, Kristin Ven Bruusgaard, and Dmitry Adamsky, to name a few.

5. Andrei Kokoshin, *Ensuring Strategic Stability in the Past and Present: Theoretical and Applied Questions* (Cambridge, MA: Belfer Center, 2011), http://belfercenter.ksg.harvard.edu/files/Ensuring%20Strategic%20Stability%20by%20A.%20Kokoshin.pdf.

6. For Russian Aerospace threat perceptions, see Lt. Col. Thomas R. McCabe, "The Russian Perception of the NATO AerospaceThreat," *Air & Space Power Journal* (Fall 2016), http://www.au.af.mil/au/afri/aspj/digital/pdf/articles/2016-Fall/V-McCabe.pdf. For the relationship between Russia's conventional weakness and its nuclear forces see Roger McDermott, "Russia's Conventional Military Weakness and Substrategic Nuclear Policy," U.S. Army, Fort Leavenworth, Kansas, 2011, http://fmso.leavenworth.army.mil/Collaboration/international/McDermott/Russia-NuclearPolicy.pdf.

7. "Gen. Baluyevsky: New Russian Military Doctrine to Have no Provisions on Preventative Nuke Strike, Potential Enemy (Part 2)," Interfax, September 5, 2014, http://www.interfax.ru/russia/395154.

Kokoshin argues that pre-nuclear deterrence should rely on highly networked, dual-capable, long-range precision-guided munitions deployed from submarines, surface ships, and long-range aircraft to strike high-value targets well beyond the conflict's front lines.[8] Influenced by Marshal Nikolai Ogarkov's Revolution in Military Affairs concept and Major-General Vladimir Slipchenko's Sixth Generation Warfare concept, these strikes would be aimed at crippling key military and national infrastructure throughout an enemy's territory.[9] Such tools would be highly effective means of inflicting significant damage at remote distances, and would be less likely to trigger unwanted escalation compared to limited nuclear use.

A pre-nuclear deterrence system is not intended to replace the threat of nuclear escalation, but to complement it and, ideally, make it more credible. Pre-nuclear deterrence is envisioned to be a credible "last warning" prior to limited nuclear use as a conflict begins to escalate to the regional or global level of war.[10] However, as noted in an article appearing in an important theoretical journal of the Russian General Staff, *Voeynna Mysl*, should this "last warning" be overlooked or ignored, "the transition to the use of nuclear weapons would be logical and inevitable."[11]

In this sense, pre-nuclear deterrence would seek to shape an opponent's risk perception in order to bring about outcomes favorable to Russia. Dmitry Adamsky, an Israeli specialist in Russian military doctrine, places this idea within the broader concept of cross-domain coercion. According to Adamsky, cross-domain coercion is a deterrence/compellence strategy that "operates under the aegis of the Russian nuclear arsenal and aims to manipulate the adversary's perception, to maneuver its decision-making process, and to influence its strategic behavior while minimizing, compared to the industrial warfare era, the scale of kinetic force use."[12] Such a strategy ties together nuclear, nonnuclear, and information capabilities into a holistic approach to manipulate an adversary's perceptions, strategic choices, and ultimately its will to act. Pre-nuclear deterrence's value would be in its psychological uses, combining capability with coercion to manipulate an adversary into believing the "military operations he launches may turn into an environmental and

---

8. Ibid.

9. For example, see Interview with Marshal of the Soviet Unition N. V. Ogarkov, "The Defense of Socialism: Experience of History and Yesterday and Today," Krasnaya Zvezda, 1st Ed., May 9, 1984 (English experts found in Lawrence R. Fink, "the Soviet View of War and Military-Technical Progress: Implications for ICBMs," *Comparative Strategy* 8 [1989]: 323–324); Vladimir Slipchenko, "Strategicheskoye neyadernoye sderzhivaniye," *Obozrevatel' Observer Zhurnal*, no. 2 (2002), http://observer.materik.ru/observer/N02_2002/2_09.htm; Alexei Arbatov, *The Transformation of Russian Military Doctrine: Lessons Learned from Kosovo and Chechnya* (Washington, DC: George C. Marshall Center, 2000), http://www.marshallcenter.org/MCPUBLICWEB/MCDocs/files/College/F_Publications/mcPapers/mc-paper_2-en.pdf.

10. Kokoshin, *Ensuring Strategic Stability in the Past and Present*. Also see A. A. Kokoshin, V. A. Veselov, and A. V. Liss, "Sdezhivaniye vo vtorom yadernom veke," Russian Academy of Science, Moscow, 2001, http://www.bestreferat.ru/referat-397232.html.

11. V. M. Burenok and O. B. Achasov, "Neyademoye sdezhivaniye," *Voyenna Mysl*, no. 12 (2007): 12–15, http://militaryarticle.ru/voennaya-mysl/2007-vm/10005-nejadernoe-sderzhivanie. English version downloaded from High Beam Research Database, December 10, 2014.

12. Dmitry Adamksy, *Cross-Domain Coercion: The Current Russian Art of Strategy*, Proliferation Papers No. 54 (Paris: Institut Francais des Relations Internationales, November 2015), http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

sociopolitical catastrophe instead of victory and attainment of the goals he sets himself."[13] As such, it appears pre-nuclear deterrence is favored not only for its destructive power, but for its capacity to compel an opponent based on the credible threat that Russia can escalate a conflict without crossing the nuclear threshold.

OPERATIONALIZING PRE-NUCLEAR DETERRENCE: CONVENTIONAL DE-ESCALATION?

Russian strategists have begun to analyze how to operationalize Kokoshin's model as an asymmetric tool vis-à-vis the United States and NATO. While there appears to be a wide range of ideas, synthesizing the literature (particularly writings from *Voeynna Mysl*) provides insight into the concept of pre-nuclear deterrence. Posited below are three intertwined and complementary functions, aimed at imposing costs on and coercing an adversary: nonviolent posturing, defensive operations, and asymmetric actions "relying on the efficiency of modern high-precision conventionally equipped strategic weapons systems."[14]

The first function of pre-nuclear deterrence can be described as deterrence through demonstration, or deterrence through intimidation.[15] This coercive mechanism weaves together information operations and nonviolent posturing (exercises, demonstrations, deployments, etc.) to intimidate an opponent prior to or during hostilities. Targeted and uninterrupted information operations (official statements/threats, leaked data, etc.) would articulate Russia's rationale for its actions and exaggerate its readiness and ability to inflict unacceptable damage against vitally important interests should an opponent take or continue to take an undesirable action.[16] In theory, such actions would present a highly credible threat and raise the stakes to an undesirable level, ultimately compelling the opponent to change course and seek cessation of a crisis. While the information aspect may be most evident here, it should be noted that the information campaign is a central factor for all three functions.

The second function, defensive operations, resembles a robust anti-access/area denial (A2/AD) capability.[17] While this may be nominally defensive, featuring advanced integrated air and missile

---

13. S. G. Chekinov and S. A. Bogdanov, "Asymmetrical Actions to Maintain Russia's Military Security," *Military Thought*, no. 1 (2010): 1–11, http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.1_2010_small.pdf.

14. Kokoshin, *Ensuring Strategic Stability in the Past and Present*; Burenok and Achasov, "Neyademoye sdezhivaniye"; V. I. Polegayev and V. V Alferov, "Nonnuclear Deterrence in the Strategic Deterrence System," *Military Thought*, no. 3 (2015): 7–15; Chekinov and Bogdanov, "Asymmetrical Actions to Maintain Russia's Military Security."

15. S. G. Chekinov and S. A. Bogdanov, "The Nature and Content of New-Generation War," *Military Thought*, no. 4 (2013), http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf; Burenok and Achasov, "Neyademoye sdezhivaniye."

16. Ibid.; Sergei Ermakov, "Yadernoye oruzhiye vytesnyayut informatsionnyye tekhnologii," *Pravda*, December 15, 2015, http://www.pravda.ru/news/expert/15-12-2014/1240108-Sergey_Ermakov-0/.

17. Burenok and Achasov, "Neyademoye sdezhivaniye"; Chekinov and Bogdanov, "Asymmetrical Actions to Maintain Russia's Military Security."

defenses to cope with NATO's advantages in airpower, it also has openly offensive elements. Indeed, Russia has sought to procure a variety of multidomain capabilities, such as anti-ship weapons, cyber technology, counter-space capabilities, and electronic warfare systems to disrupt enemy counteroffensives and hold at risk a range of military infrastructure throughout the immediate battlefield and theater of war.[18] These options afford Moscow greater ability to challenge NATO without crossing the nuclear threshold. During a conflict, nonnuclear capabilities can cripple an enemy's key installations, allowing Russia to offset a superior force.[19] Strikes can be conducted from multiple directions, often without having to leave Russian territory. Should Russia attempt an aggressive fait accompli against a NATO member, strikes against alliance pressure points, such as transportation hubs, bases, and command and control (C2) could inhibit the alliance's ability to dislodge Russian forces after they seize territory.[20]

The third function envisions the use of long-range nonnuclear strikes and potentially new technologies to inflict unacceptable damage against critically important civilian facilities to coerce and intimidate.[21] Unlike defensive operations, this function aims to produce "measureable economic damage to the aggressor" and its society through destruction of civilian politico-economic infrastructure deep within an adversary's territory.[22] According to some Russian analysts, this can be accomplished by destruction of nuclear power plants, hydroelectric dams, and other critical infrastructure to trigger catastrophic economic and ecological effects.[23] Yet despite imposing

---

18. Stephen Blank, "Imperial Ambitions: Russia's Military Buildup," *World Affairs* (May/June 2015), http://www.worldaffairsjournal.org/article/imperial-ambitions-russia%E2%80%99s-military-buildup.

19. Victor Saksonov, "Neyadernoye sderzhivaniye," *Nezavisimoye Voyennoye Obozreniye*, August 12, 2016, http://nvo.ng.ru/realty/2016-08-12/7_rocket.html.

20. Polegayev and Alferov, "Nonnuclear Deterrence in the Strategic Deterrence System."

21. Most Russian analysts, including Kokoshin, posit long-range conventional strike systems will accomplish this goal. Less clear is the role other technologies, such as space and cyber, may play. Given Russia's interest in leveraging asymmetric capabilities, additional tools are likely to be used in the pre-nuclear phase. For example, cyber attacks could be used to cripple critical infrastructure while antisatellite operations could degrade valuable space infrastructure. As other technologies emerge, they may also play a role in pre-nuclear deterrence. As such, pre-nuclear deterrence does not rely solely on long-range conventional strike, but an assortment of nonnuclear, strategic capabilities. B. N. Kuzyk, *Vybor Veka*, 2nd ed. (Moscow: Institute for Economic Strategies, 2004), 199–213, http://www.kuzyk.ru/upload/objects/docs/1120641832_glava7.pdf; Kokoshin, *Ensuring Strategic Stability in the Past and Present*; Burenok and Achasov, "Neyademoye sdezhivaniye"; Chekinov and Bogdanov, "Asymmetrical Actions to Maintain Russia's Military Security"; and Chekinov and Bogdanov, "The Nature and Content of New-Generation War."

22. Vladimir Frolov, "The Arms Race Goes Global," *Moscow News*, November 2, 2006; Kuzyk, *Vybor Veka*; Dmitry Rogozin, et. al., "Strategiya sderzhivaniya: i novyye vidy yadernogo strategicheskogo oruzhiya," in *Voyna i mir v terminakh i opredeleniyakh*, ed. Dmitry Rogozin, http://www.voina-i-mir.ru/chapter/11; Kokoshin, *Ensuring Strategic Stability in the Past and Present*, 58; Chekinov and Bogdanov, "Asymmetrical Actions to Maintain Russia's Military Security"; and Chekinov and Bogdanov, "The Nature and Content of New-Generation War."

23. Konstantin Sivkov, "Russkiy global'nyy udar," *Voyenno-promyshlennyy kur'yer*, no. 2 (January 2014), http://vpk-news.ru/articles/18829; Leonid Ivashov, "Russia Must Keep USA at Gunpoint," *Pravda*, December 1, 2015, http://www.pravdareport.com/russia/politics/12-01-2015/129505-russia_usa_war-0/; Chekinov and Bogdanov, "Asymmetrical Actions to Maintain Russia's Military Security"; Chekinov and Bogdanov, "The Nature and Content of New-Generation War."

significant damage, Russian military theorists hold such strikes would not "rob the adversary of the alternative to de-escalate" the conflict.[24]

Such thinking outlines a Russian pre-nuclear "theory of victory," which relies on the threat of escalation to radically transform the nature of a conflict and compel an opponent to manage hostilities. Although this strategy is often linked to Russia's regional nuclear doctrine, Moscow also appears to see a nonnuclear component.[25] Indeed, Russian pre-nuclear strategy fits neatly into Russian concepts of conflict management and cross-domain coercion. How long the pre-nuclear phase would last and the actual conditions under which Russia might execute it are uncertain. During an escalating crisis or military conflict, the decision to strike critical nonmilitary targets in NATO will likely be profoundly influenced by the military situation as well as the attitudes of those individuals advising the Russian president. Domestic political factors will be important as well, perhaps as important as military considerations. Looking to convey resolve and risk in the hopes of sustaining advantage—or avoiding defeat—in an escalating conflict, these advisers may well see nonnuclear options that have the potential to achieve strategic results as a more tolerable escalation option than recourse to the limited use of nuclear weapons.

LONG-RANGE CONVENTIONAL STRIKE: DERIVING PRE-NUCLEAR DETERRENCE BENEFITS IN SYRIA?

The Russian military intervention in Syria has provided an opportunity for the Kremlin to test some of its new systems under actual combat conditions, including those associated with pre-nuclear deterrence.[26] Perhaps the most interesting example regarding these latter types of capabilities is recent Russian employment of long-range, nonnuclear cruise missiles against targets that would be included in pre-nuclear target sets.[27] Beginning in October 2015, Russia has launched several salvos of ship- and submarine-launched Kalibr cruise missiles, as well as Kh-555 and Kh-101 air-launched cruise missiles (ALCMs) from strategic bombers, to destroy Islamic State and Al Nusra targets in Syria.[28] According to Russian press reports, operations have included command centers,

---

24. Polegayev and Alferov, "Nonnuclear Deterrence in the Strategic Deterrence System."

25. See ibid. Also see "The Priority Tasks of the Development of the Armed Forces of the Russian Federation," Defense Ministry of the Russian Federation, 2003, http://red-stars.org/doctrine.pdf.

26. Vincent R. Stewart, "Worldwide Threat Assessment" (statement before Senate Armed Services Committee, February 9, 2016), http://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/653278/statement-for-the-record-worldwide-threat-assessment/.

27. "Russian Caspian Fleet, Syria Air Group, Carrying Out More Strikes—Minister," BBC Monitoring of the Former Soviet Union, *Lexis Nexis,* November 20, 2015; Ivan Safronv, "V nebesakh i na more," *Kommersant*, November 30, 2015, http://www.kommersant.ru/doc/2862703.

28. "Russian Aviation Destroys Three Major Oil Facilities in Syria—General Staff," Itar-Tass, November 19, 2015, http://tass.ru/en/defense/837869; "Twenty-Nine Long-Range Aircraft Deliver Strikes at IS Facilities from Russia—Minister," Itar-Tass, November 20, 2015, http://tass.ru/en/defense/838198; "Russia's Newest Weapons Used in Syria for the First Time," *Sputnik News*, November 20, 2015, http://sputniknews.com/military/20151120/1030459883/tu160-strategic-bomber-kh101-su34-cruise-missiles.html.

ammunition dumps, and oil infrastructure.[29] The strikes were considered highly successful, despite reports that at least four Kalibr missiles malfunctioned and crashed in Iran.[30]

These operations raised questions as to why it was necessary to employ sophisticated standoff munitions against a far less capable adversary. To be sure, the strikes gave Russian commanders an opportunity to assess capabilities and concepts under the strain of genuine conflict. But continued strikes are an expensive test of Russia's limited cruise missile stocks. A more convincing theory suggests that such operations may also be aimed at shaping Western perceptions of Russian capability, or an attempt at deterrence by demonstration/intimidation.

Indeed, the subsequent intimidation campaign was unmistakable, as cruise missile strikes in October 2015 were followed by a flood of Russian media reports.[31] Articles and video documentaries all helped convey a picture of Russia's growing lethality and its credible challenge to NATO. Indeed, one report went so far as to suggest the 26 cruise missiles launched from the Caspian in early October were intended to represent the 26 European members of NATO vulnerable to Kalibr cruise missile strikes.[32] Other accounts reached a similar conclusion: Russia has broken the West's monopoly on efficiently employing long-range precision strikes, greatly increasing NATO's vulnerability.[33]

The Putin administration and the military were also active in crafting this narrative. During an interview with a Russian television channel, President Vladimir Putin asserted cruise missile strikes in Syria were meant to demonstrate "Russia has the will to use them [long-range cruise missiles] if it satisfies the national interests of our state and our people."[34] The Defense Ministry posted videos of cruise missile strikes to their website and social media accounts, while top commanders lauded Russia's new long-range munitions. The Russian military also acknowledged that NATO should take note of Russia's growing capabilities. For example, Vice Admiral Viktor Bursuk, deputy command-in-chief of the Russian navy, told *Interfax* reporters, "The range of these missiles [Kalibr] allows us to say that ships located in the Black Sea can destroy targets in quite distant regions, which was an unpleasant surprise for NATO countries."[35]

---

29. "Russian Defense Ministry Praises Kalibr Sea-Launched Missiles Used against IS Targets," ITAR-TASS, December 9, 2015, http://tass.com/defense/842799.

30. Barbara Starr and Jeremy Diamond, "US Officials Say Russian Missiles Heading for Syria Landed in Iran," CNN, October 8, 2015, http://www.cnn.com/2015/10/08/politics/russian-missiles-syria-landed-iran/.

31. Ivan Safronv, "V nebesakh i na more," *Kommersant*, November 30, 2015, http://www.kommersant.ru/doc/2862703; "Russia's Newest Weapons Used in Syria for the First Time," *Sputnik News*, November 20, 2015, http://sputniknews.com/military/20151120/1030459883/tu160-strategic-bomber-kh101-su34-cruise-missiles.html.

32. Oleg Vladykin, "V armii. Rossiya obladayet krylatymi raketami dlya naneseniya global'nogo udara," *Nezavisimoye Voyennoye Obozreniye*, October 11, 2015, http://www.ng.ru/week/2015-10-11/11_army.html.

33. Kirill Voronkov, "REAL'NAYA zona pokrytiya krylatymi raketami Kalibr-NK," *Live Journal*, October 8, 2015, http://voronkov-kirill.livejournal.com/138347.html.

34. "In Putin's Own Words: Why We Launched Kalibr Missiles," *7 Feet beneath the Keel Blog*, October 12, 2015, http://7fbtk.blogspot.com/2015/10/in-putins-own-words-why-we-launched.html.

35. "New-Generation Corvettes Equipped with Kalibr-NK Missiles to Join All Russian Fleets—Navy Deputy Commander," Interfax, October 23, 2015, http://www.interfax.com/newsinf.asp?id=628193.

These types of statements make it appear that the Kalibr and Kh-101 launches were carried out to achieve strategic effects, both militarily and psychologically, well beyond the Syrian theater of conflict.[36] For the Kremlin, the prospect of influencing NATO's strategic calculus was (and continues to be) a key contribution of ongoing cruise missile strikes in Syria. From Moscow's vantage point, this not only offers some immediate benefits in and out of theater (strikes in Syria could deter coalition threats to the Assad regime and potentially NATO interference in Ukraine simultaneously), it also works to precondition an adversary's perceptions for future confrontations. It does so by demonstrating Russia's willingness and capability to increase the risk and pain to an opponent by employing new systems for long-range conventional strikes—a coercive lever previously lacking.

Russia's operations in Syria, however, have not helped clarify the relationship between pre-nuclear deterrence and the nuclear threshold. In theory, pre-nuclear deterrence, as described in Russian military journals, utilizes sophisticated nonnuclear capabilities to deter an opponent and thereby reduce Russian reliance on nuclear threats. In practice, Russian actions in Syria have demonstrated a tendency toward continuing to link conventional and nuclear deterrence. For example, Putin himself confirmed the long-range cruise missiles used in Syria were nuclear-capable.[37] The Russian military also bolstered the image of close conventional-nuclear coordination by conducting exercises that featured dual-capable Iskander tactical ballistic missiles and Kalibr cruise missiles, as well as submarine-launched cruise missile (SLBM) and ICBM launches.[38] Such linkages suggest Russian leaders continue to rely on nuclear forces to deter capable opponents and are wary of the degree to which they can depend on nonnuclear deterrence, even as they continue to develop capabilities and concepts associated with the latter. As such, pre-nuclear capabilities appear to have retained a close relationship with nuclear weapons despite the interests and efforts of Kokoshin and other Russian strategists to reduce Russia's present reliance on nuclear weapons to counter real and perceived gaps with regard to its conventional forces.

PRE-NUCLEAR DETERRENCE FOUNDATIONAL ASSUMPTIONS: A CRITICAL ASSESSMENT

This Russian "theory of victory" at the high-end spectrum of conventional conflict is constructed around underlying assumptions on the nature of a conflict, the opponent to be deterred, and what that opponent values. For Russian strategy to be successful, most, if not all assumptions must prove accurate. Based on the previous analysis, these assumptions can be discerned and critically assessed.

---

36. David Blair, "Russia Sends Warning to West with Show of Strength in Syria," *Telegraph*, December 13, 2015, http://www.telegraph.co.uk/news/worldnews/europe/russia/12047257/Russia-sends-warning-to-West-with-show-of-strength-in-Syria.html.

37. Meeting with Defence Minister Sergei Shoigu, Kremlin, Moscow, December 8, 2015, http://en.kremlin.ru/events/president/news/50892.

38. Pavel Podvig, "Russia Tests Command and Control System in an Exercise with Multiple Missile Launches," *Russian Forces Blog*, October 30, 2015, http://russianforces.org/blog/2015/10/russia_tests_command_and_contr.shtml.

First, Russia expects a favorable asymmetry in the stakes during a future notional NATO-Russia conflict. As noted by Brad Roberts, according to Russian views, "the asymmetry of stakes favors Russia because any conflict between NATO and Russia would jeopardize vital Russian interests, whereas it would involve important but not vital NATO or U.S. interests."[39] This view is underpinned by the likelihood that a Russian-NATO confrontation would evolve from a localized war along Russia's periphery. The territory in question is likely to have cultural, historic, or ethnic ties (or all three) to Russia.[40] Conversely, such battlefields may be distant and foreign to most NATO members. The inherent asymmetry in geography further reinforces Moscow's assumptions. For example, Russia can project power into the Baltics from the safety of its territory, whereas NATO would likely require substantial forces from Western Europe and the United States.[41] As a result, Russia assumes it would hold far more equity in a confrontation, and would fight harder, longer, and endure higher costs than NATO.

Second, Russian perceptions are premised on an assessment of NATO's military power and preparedness.[42] Due to NATO's aggregate military dominance, pre-nuclear deterrence seeks to exploit gaps in the latter, capitalizing on the imbalance of force levels and readiness in Eastern Europe. By exploiting tactical and operational advantages in rapid mobility, layered defenses, and offensive strike capability, Russia can deny large-scale mobilization, rapid reinforcement, and decisive effects from standoff airpower. An allied breakthrough would only come at a high cost of blood and treasure, placing the burden of escalation onto the alliance. Rather than risk a protracted conflict, Russian strategy appears confident that some, perhaps even most, NATO members would seek conciliation.

Third, Russian experts assume targeting NATO's civilian infrastructure can also slow, complicate, and perhaps even halt an effective alliance response. A broad strain of Russian military literature envisions degrading an opponent's critical infrastructure as a means to inflict significant and cascading damage across the full spectrum of a state's government services and economic functions to avoid or forestall a military-to-military conflict that Russia is not sure it can win.[43] For example, in 2007 Admiral Vladimir Masorin, commander-in-chief of the Russian navy, observed that advanced world economies were susceptible to systemic disruption, writing that "the

39. Roberts, *The Case for Nuclear Weapons in the 21st Century*, 134.

40. See Jānis Bērziņš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, Policy Paper No. 2 (Riga: National Defence Academy of Latvia, April 2014), http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx.

41. For example, nonnuclear ALCMs Raduga Kh-555 and Kh-101 reportedly boast a range around 5,000 to 6,000 kilometers, while the Kalibr SLCM has a reported operational range of 2,500 kilometers. See "Russian Air Force to Get New Cruise Missile in 2013," *Sputnik News*, September 26, 2012, http://sputniknews.com/military/20120926/176233341.html; and "The Russian Navy: A Historic Transition," Office of Naval Intelligence, December 2015, http://www.oni.navy.mil/Portals/12/Intel%20agencies/russia/Russia%202015print.pdf?ver=2015-12-14-082038-923.

42. Paul Bernstein and Deborah Ball, "Putin's Russia and US Defense Strategy," Workshop Report, Air University, August 19–20, 2015, http://www.au.af.mil/au/cpc/pdfs/Putins-Russia-and-US-Defense-Strategy.pdf.

43. James Bosbotinis, "Russian Long Range Aviation and Conventional Strategic Strike," Defence iQ, March 5, 2015, http://www.defenceiq.com/air-forces-and-military-aircraft/articles/russian-long-range-aviation-and-conventional-strat; "The RF Navy vs Your 'Critically Important Facilities,'" *7 Feet beneath the Keel Blog*, March 29, 2015, http://7fbtk.blogspot.com/2015_03_01_archive.html; Sivkov, "Russkiy global'nyy udar"; Kuzyk, *Vybor Veka*.

interdependence of national economies at the world level makes it possible, by affecting the economy of one or several countries, to trigger off unacceptable economic vacillations or crises in the entire coalition of potential adversaries."[44] Other Russian experts note in *Voeynna Mysl* that any European country has a large number of objectives vitally important for the survival of a state and its population, the destruction of which can lead to unacceptable damage and force an enemy to cease military operations on terms favorable for Russia.[45] Indeed, Admiral Chirkov, recently retired commander and chief of the Russian navy, seemingly acknowledged this philosophy, stating that new conventional long-range strike capabilities enable the Russian navy to "[solve] the problem of strategic non-nuclear deterrence by the threat of destruction of critical military and *economic targets of the enemy*."[46]

The final premise is that nuclear threats can ultimately guarantee that any conflict with NATO or the United States would remain limited, likely in a manner that suits Russian tactical and strategic objectives. As noted by Forrest Morgan, "Whereas strategic parity made Cold War leaders cautious, it could lead today's leaders to place more faith in stability than is warranted. Moscow might gamble on hopes that fears of escalation would make the West shy of confronting a Russian military intervention."[47] Here, the Russian expectation is that the nuclear shadow would be ubiquitous and its dangers salient. By raising the nuclear specter, Moscow presumes to manipulate NATO's perception of risk to disincentivize a counter-response. In this context, the actual degree to which pre-nuclear deterrence is integrated within Russian nuclear planning is less important; rather, Russian nuclear weapons are a universal reminder to NATO that any conflict with Russia could potentially escalate past the nuclear threshold.

These insights reveal an implicit but central Russian judgment about NATO's resolve. Evidently, Russian experts view NATO as risk-averse, subject to manipulation, and unlikely to tolerate significant loss of blood and treasure over interests vital to Russia. Tailored damage against important civilian and military infrastructure, coupled with Russian readiness to escalate a conflict up to, and perhaps past, the nuclear threshold, would induce a sense of vulnerability, overshadowing any benefits of a major conflict.[48] Rather than risk conflict intensification, the imbalance in the stakes and Russia's willingness to escalate would exploit fissures in alliance cohesion and prompt NATO members to seek a negotiated peace (or at least fail to rally to the defense of a beleaguered ally), thereby terminating a conflict without having to resort to nuclear use.

---

44. Vladimir Masorin, "Morskaya doktrina kak sostavnaya chast' voyennoy doktriny," *Voeynna Mysl*, no. 3 (2007), found in James Bosbotinis, "The Russian Federation Navy: An Assessment of Its Strategic Setting, Doctrine and Prospect," Defence Academy of the United Kingdom, September 2010, http://www.admiraltytrilogy.com/read/Russian_Navy_Prospects.pdf.

45. Chekinov and Bogdanov, "Asymmetrical Actions to Maintain Russia's Military Security."

46. "VMF Rossii nadeyetsya rezko uvelichit' boyesposobnost' za schet robotov i iskusstvennogo intellekta," Interfax, December 19, 2012, http://www.interfax.ru/russia/281757; Anastasia Petrova, "Ot robotov do avianostsev," *Vzglyad Gazeta*, December 19, 2012, http://vz.ru/society/2012/12/19/612765.html. Emphasis added.

47. Forrest E. Morgan, *Dancing with the Bear: Managing Escalation in a Conflict with Russia*, Proliferation Papers (Paris: Institut Francais des Relations Internationales, Winter 2012), 36, http://www.ifri.org/sites/default/files/atoms/files/pp40morgan.pdf.

48. A. L. Khryapin and V. A. Afanasyev, "Conceptual Principles of Strategic Deterrence," *Military Thought*, no. 1 (2005).

These baseline assumptions, however, are flawed. Pre-nuclear deterrence posits an ability to understand an economically and politically vulnerable enemy's pain thresholds and manipulate its cost-benefit calculus, while clearly communicating Russian intentions and vital interests. Yet Russian leaders may misjudge the coercive utility of pre-nuclear deterrence and miscalculate an adversary's likelihood to abandon a crisis or hostilities. The stakes may not innately favor Russia, as threats to NATO's Article V commitments could exacerbate members' perceptions of risk and strengthen their determination. Moreover, destruction of political-economic civilian infrastructure in a NATO state, particularly in North America, would undoubtedly be viewed by Western leaders as highly aggressive and escalatory. Rather than acquiesce to Russian actions, a strategic non-nuclear attack may actually unite NATO members into bringing the full potential of the alliance to bear, shifting the nature of the conflict from a localized crisis to a major regional war. Such a development would likely only increase pressure (due both to external and internal concerns) on Russian decisionmakers, compelling Russian leaders to turn to the threat, or perhaps even limited employment, of nuclear weapons to avoid defeat or prolong war. Should Russia overestimate an imbalance in stakes and underestimate alliance solidarity or NATO's willingness to absorb losses, pre-nuclear deterrence is very likely to fail.

CONCEPTUALIZING A NATO PRE-NUCLEAR OFFSET

How should NATO respond to Russian pre-nuclear deterrence? This section uses the long-standing 2006 Department of Defense *Deterrence Operations Joint Operating Concept* (DO JOC) to outline the beginnings of a countervailing NATO deterrence strategy. The DO JOC describes how to conceptualize tailored deterrence strategies at the operational level. Its framework posits three successive elements: ends, ways, and means.[49] According to the DO JOC, "In order to achieve these objectives (ends), joint forces must be able to employ various capabilities (means) to undertake operations and activities (ways) that can decisively influence the decision-making calculus of key adversary decision-makers."[50] This provides a useful methodology for framing requirements tailored to deter Russian strategy.

The starting point for any military framework should begin with the ends or objectives the political leadership wishes to achieve. At the pre-nuclear rung, NATO's fundamental objective should be to decisively influence Russian decisionmaking calculus that high-intensity attacks are futile, self-defeating, and costly. As outlined by the DO JOC, Russian leaders must be convinced that pre-nuclear courses of action would "result in outcomes that are decisively worse than they could achieve through alternative courses of action available to them."[51] NATO activities should be visible and credible, conveying to Russia it cannot dictate the terms of a conflict. The strategic

49. Department of Defense (DoD), *Deterrence Operations Joint Operating Concept*, Version 2 (Washington, DC: DoD, 2006).

50. For example, the DO JOC describes how a U.S. JFCwill plan, prepare, deploy, employ, and sustain a joint force to achieve deterrence objectives set forth by the national leadership of the United States. DoD, *Deterrence Operations Joint Operating Concept*, 19.

51. Ibid., 23.

message should be equally clear: NATO is able to respond quickly and effectively to any level of violence.

Achieving this objective requires ways or supporting concepts to connect strategic goals to appropriate capabilities. Successfully influencing Russian decisionmaking results in part from two traditional deterrence concepts: "The capabilities to deny an aggressor the prospect of achieving his objectives and from the complementary capability to impose unacceptable costs on the aggressor."[52] These concepts are recognized as deterrence by denial and deterrence by punishment. Given the wide range of Russian objectives at the pre-nuclear level, NATO requires both concepts to impact the decisionmaking calculus of Russian political and military leadership. Denying benefits ensures Russia cannot be certain its operations will be successful at a reasonable cost. Imposing costs convinces the Russian leadership that it cannot achieve a quick, decisive, and inexpensive victory.[53]

Both deterrence concepts require a suite of military capabilities tailored to achieve decisive influence over Russian strategic calculus. Visible military capabilities provide tangible insight into the seriousness of NATO's intent, ultimately underwriting deterrence in the conventional space.[54] Should deterrence fail, these capabilities can help encourage restraint and contribute to conflict termination. In this context, capability is fungible with credibility to some extent.[55] Although statements or actions can help reinforce deterrence, "they do not contain inherent credibility."[56]

Thus, NATO must evaluate whether the alliance maintains the proper mix of high-end capabilities to achieve its objective of deterring Russian pre-nuclear operations. As noted by the 2012 NATO Deterrence and Defence Posture Review, "The Alliance must be able to address the full spectrum of current and future challenges and threats from any direction, simultaneously. It is therefore strengthening its deterrence and defence posture in view of the changed and evolving security environment."[57] But NATO's conventional advantages—the cornerstone of NATO deterrence—are under increasing stress. Russian pre-nuclear theories and capability demonstrations reveal a desire to leverage high-end capabilities and asymmetric tactics to offset NATO conventional dominance. In addition, NATO defense retrenchment and reorientation have atrophied a number of key capabilities relevant to deterring a well-equipped state adversary.[58] The perceptions of NATO's diminishing conventional superiority are likely to exacerbate questions over NATO's credibility, from allies and adversaries alike.

---

52. DoD, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: DoD, January 2012), 4, http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf.

53. Michael S. Gerson, "Conventional Deterrence in the Second Nuclear Age," *Parameters* 39, no. 3 (Fall 2009), http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/09autumn/gerson.pdf.

54. Ibid.

55. Clark A. Murdock and Jessica M. Yeats, *Exploring the Nuclear Posture Implications of Extended Deterrence and Assurance: Workshop Proceedings and Key Takeaways* (Washington, DC: CSIS, November 2009), 1, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100222_Murdock_NuclearPosture_Print.pdf.

56. Robert Jervis, *The Logic of Images in International Relations* (Princeton, NJ: Princeton University Press, 1970), 21.

57. NATO, "Deterrence and Defence Posture Review," press release, May 21, 2012, http://www.nato.int/cps/en/natohq/official_texts_87597.htm.

58. Bernstein and Ball, "Putin's Russia and US Defense Strategy."

FORCE POSTURE PROPOSALS FOR HIGH-END NONNUCLEAR DETERRENCE

The previous section linked NATO's deterrence goals with a specific requirement for capabilities at the pre-nuclear level. NATO requires a suite of capabilities tailored for high-end conflict with Russia. There are at least four areas critical to this requirement: passive defenses; active defenses; intelligence, surveillance, and reconnaissance (ISR); and long-range strike.

First, NATO can address its ability to deny benefits from an adversary waging sustained, high-intensity operations against NATO infrastructure. Given the importance of targeting infrastructure in Russian theoretical writings, augmenting key nodes with passive defenses may dissuade or minimalize benefits from aggressive actions. Latent protective measures could take several diverse, yet mutually supportive, steps in space, cyberspace, and structural resiliency. For example, the alliance could better harden critical air base elements, such as individual fighter shelters or operational facilities (fuel, munitions, etc.). Russia would need to employ more munitions per salvo to neutralize a target, potentially depleting its inventory sooner than desired.

However, excessive hardening would be cost-prohibitive. To mitigate additional risks, NATO could better disperse forward operating bases (FOBs) and information systems. One example could include small, prepositioned shell bases that could serve as modular resource hubs to replenish transient forces moving across the battlespace.[59] In space, NATO could employ greater numbers of smaller, less expensive satellites. Such dispersion would stress Russia's ISR capabilities by forcing Russian forces to account for more targets.

Second, NATO should study whether active defenses to repel adversary actions can and should play a larger role in NATO's deterrence posture. Overspecialization in counterinsurgency warfare has impacted active defense investment in critical capabilities, such as air defense, antisubmarine warfare, and electronic warfare.[60] Fielding these capabilities would enable NATO to more aggressively disrupt Russian aerospace and sub-surface threats.

A more contentious decision would be whether NATO's missile defense shield should be re-oriented toward Russian short- and intermediate-range ballistic missile and cruise missile threats. NATO has so far resisted calls to modify its missile defense policy. Indeed, any change in policy intended to provide defense against any type of Russian system would be seized upon by Moscow as proof that NATO's missile defenses were always intended for Russia (and, in particular, are ultimately intended to negate Russia's nuclear deterrent).[61] Yet missile defenses may offer important

---

59. For example, this could take the form of what the Air Force calls untethered operations. See Maj. Gen. Charles Q. Brown, Brig. Gen. Bradley D. Spacy, and Capt. Charles G. Glover III, "Untethered Operations," *Air & Space Journal* 28, no. 3 (May–June 2015), http://www.au.af.mil/au/afri/aspj/digital/pdf/articles/2015-May-Jun/SLP-Brown_Spacy_Glover.pdf.

60. For example, see Sydney J. Freedberg Jr., "Russia Builds 'Arc of Steel': Adm. Ferguson," *Breaking Defense*, October 6, 2015, http://breakingdefense.com/2015/10/russia-builds-arc-of-steel-adm-ferguson/.

61. The narrative has now also expanded to include the Aegis Ashore ballistic missile defense systems in Romania and Poland. They are also able to employ land-attack Tomahawk cruise missiles. In addition to a highly aggressive posture, Russia holds this is a blatant violation of the 1987 Intermediate-Range Nuclear Forces Treaty, which prohibits land-based missiles between 500 and 5,000 kilometers.

benefits in mitigating cruise and ballistic missile volleys. Before moving forward, NATO would need to consider at least six important questions:

- What impact might reorienting missile defense policy have on alliance cohesion?
- What attributes does an augmented missile defense shield require?
- Do missile defenses add relatively more deterrent and war-fighting value than additional offensive forces?
- How effective might a missile defense structure be against Russian salvos?
- How should reoriented missile defenses be postured? What critical nodes should be defended?
- What is the likely Russian response?

Third, NATO will need to assess its ability to meet demand for force-multiplier capabilities, above all ISR. Robust ISR is fundamental for effective operational and tactical situational awareness, precision targeting, strategic foresight, and early warning—all of which would be under considerable stress during a high-end conflict.[62] Without accurate and timely ISR, any strike against Russian networks or systems would be highly problematic.[63] This reality should lead the alliance to consider ISR augmented for contested environments.

Three important ISR attributes are essential for nonpermissive environments: quantity, survivability, and robust data processing. First, NATO requires sufficient assets to support a high-end operation against Russia. Sustained European ISR investment and procurement could help mitigate expected shortages while reducing overreliance on the United States. Second, ISR should be survivable. Contrasting with the permissive environments in Afghanistan, Iraq, and Libya, Russia employs a panoply of disruptive capabilities to inhibit NATO ISR collection.[64] A renewed focus on platforms and transmission systems optimized for A2/AD environments could partially address survivability concerns. Specifically, NATO could invest in stealthy penetrating ISR platforms and advanced datalink security. Finally, ISR should encompass robust data processing. Without efficient processing, exploitation, and dissemination (PED), timelines between identification to destruction become prolonged and operations ineffective. NATO will need to continue to develop more efficient mass data processing and rapid dissemination under its evolving joint ISR initiatives.[65]

Lastly, NATO will also need to reassess its capability to impose costs on Russian forces and networks. Imposing costs demands projecting power into contested zones and Russian territory

62. Dominik Jankowski, "The Alliance on Its Road from Warsaw to Brussels," European Geostrategy, September 1, 2016, http://www.europeangeostrategy.org/2016/09/the-alliance-on-its-road-from-warsaw-to-brussels/.

63. Kathleen H. Hicks et al., *Evaluating Future U.S. Army Force Posture in Europe: Phase II Report* (Washington, DC: CSIS, 2016), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160712_Samp_ArmyForcePostureEurope_Web.pdf.

64. This includes physical attacks, interference (electromagnetic, cyber, and space jamming, spoofing, dazzling, etc.), and traditional deception and camouflage techniques.

65. See Matthew J. Martin, "Unifying Our Vision: Joint ISR Coordination and the NATO Joint ISR Initiative," *Joint Force Quarterly* 72 (2014), http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-72/jfq-72_54-60_Martin.pdf?ver=2014-03-13-152411-000.

through the use of capabilities such as standoff conventional systems.[66] Negating Russia's ability to constrain NATO's standoff strike potential would enhance NATO's credibility. Currently, NATO is almost completely dependent on air forces and aviation assets to project power and conduct standoff missions.[67] This is particularly disconcerting given NATO airpower's growing vulnerability to Russian long-range strike, cyber, and integrated air defense systems.

Beyond augmenting the air force with greater quantities of sophisticated aircraft and precision munitions, NATO could mix other domains into a joint long-range strike mission. A lethal combination of multidomain, multivector attacks would significantly complicate Russian force calculus and provide the alliance the means to quickly retaliate, while avoiding single points of capability or capacity failure.[68] This could include ground-based systems (ATACMs, cruise and ballistic missiles, precision artillery) and sea-based systems (attack submarines, surface ships). These systems could be leveraged with other specialized assets (Special Forces, offensive cyber capabilities, and stealthy attack unmanned systems) to synergistically neutralize Russian air defense networks and supporting sensors, potentially rendering Russian ground or naval forces engaged in offensive operations much more vulnerable and, perhaps most importantly, preventing Russian strategists from assuming that any initial strike could result in a fait accompli.

CONCLUSION

As outlined in this paper, Russian theoretical debates suggest analysts are becoming more confident in leveraging high-end conventional capabilities to achieve Russian strategic objectives in the event of an armed confrontation or conflict with a modern military opponent or alliance. Apparently, this includes the role such weapons can play in deterrence and war fighting, by granting Moscow a range of additional conventional options for the purposes of escalation control and war termination. Such options would be advantageous from a Russian perspective, because they allow Russia to impose its will without crossing the nuclear threshold. However, the Russian assumptions underpinning its potential employment of these weapons—particularly with regard to economic targets—suggest Moscow may be overlooking or ignoring the potential escalation consequences of its actions. Nevertheless, NATO should be prepared to reassess its own force posture to preserve deterrence against a highly capable state adversary, such as the Russian Federation. This may include augmenting its forces with additional active and passive defenses, ISR, and standoff conventional strike assets. To be sure, pre-nuclear deterrence is not a game changer. However, it does pose new challenges to NATO, challenges the alliance needs to take seriously. Without proper understanding of the threat, the alliance is left vulnerable to shock and surprise, which could have disastrous effects on NATO military operations and the long-term prospects for peace and stability in Europe.

66. Key attributes should include survivability, promptness, and standoff range, among others.

67. Dave Majumdar, "Can America Crush Russia's A2/AD 'Bubbles'?," *National Interest*, June 29, 2016, http://nationalinterest.org/blog/the-buzz/can-america-crush-russias-a2-ad-bubbles-16791.

68. Ibid.; Mark Gunzinger and Jacob Cohn, "How to Secure NATO's Frontline States," *Breaking Defense*, August 3, 2016, http://breakingdefense.com/2016/08/how-to-secure-natos-frontline-states/.

Combatting WMD Terrorism: Law, Politics, and Flexibility of the UN Security Council Resolution 1540

Sarah Shirazyan[1]

Whether it is Islamic State of Iraq and Syria (ISIS) militants using mustard agents against Kurdish forces, Islamic extremists in Paris trying to obtain radioactive materials from Belgian nuclear facilities to make a dirty bomb, or a group of middlemen trafficking highly enriched uranium through Moldova, proliferation of weapons of mass destruction (WMD) remains a serious threat to international peace and security. To address this threat, in 2004, the United Nations (UN) Security Council enacted an unprecedented counterproliferation instrument—Resolution 1540. To facilitate and monitor countries' domestic implementation of the resolution, the Council also established an ad hoc subsidiary body—the 1540 committee—consisting of all members of the council.

This paper analyzes how the UN Security Council defined and interpreted its 1540 legal mandate to accommodate competing political pressures and organize the global fight against WMD terrorism. By examining the Resolution 1540's inception and the early strategic choices of the 1540 committee, this paper describes how institutions change at a time of great crisis. The analysis shows that the committee has chosen not to become a UN sanctions regime, either in the name of nonproliferation or counterterrorism. Instead, from the very beginning, it shaped its identity as a voluntary and cooperative mechanism. While the cooperative character of the committee generated a strong political consensus among UN member states for supporting Resolution 1540's goals, this institutional design has also placed some limits on the United Nations' ability and resources to identify and close transnational proliferation gaps.

---

1. Sarah Shirazyan is a Doctor of Science of Law (JSD) candidate at Stanford Law School, specializing in international law and international relations, with a focus on nuclear and national security law. Previously, Ms. Shirazyan worked at the Nuclear Weapons Branch of the UN Office for Disarmament Affairs, European Court of Human Rights, and the Drugs and Organized Crime Directorate of INTERPOL.

POLITICAL AND HISTORICAL CONTEXT

The rise of Islamic fundamentalism and the subsequent terrorist attacks of 9/11 have dramatically reshaped the American conception of its national security. A foreign attack on a domestic target was hardly foreseen before.[2] While the hijackers in the 9/11 attacks caused harm by using box cutters, mace, and 19 airline tickets, the 9/11 attacks amplified concerns over terrorists resorting to deadlier weapons. America faced a new and different kind of threat—one that rested at the intersection of *radicalism* and *technology*—that is, radical extremists armed with WMDs, particularly with nuclear weapons.[3] The nature of this new proliferation threat was twofold, displaying a complicated nexus between traditional state-to-state proliferation and non-state actor proliferation. First, there was a need to address nuclear pursuits of rogue states that were of a security concern to the United States, particularly Iraq.[4] Second, according to the George W. Bush administration, the terrorist groups were able to carry on their criminal activities primarily because failing and rogue states had created safe havens for them and provided operational support to terrorists.[5] Extrapolating from rogue regimes' previous behavior of supporting terrorists, there was a risk that these states could provide WMD materials to terrorist groups.

This emerging threat posed a particular challenge to the existing domestic and international arms control regimes. Existing regulatory and enforcement structures were not designed to address non-state actor nuclear proliferation. Because the new adversary was a loose group of individuals ready to die in the pursuit of their cause, the Cold War balance of power and nuclear-deterrent strategies could not work. A fundamentally new strategic response was required to address emerging proliferation threats—one that could combine both counterterror and counterproliferation policies. With that in mind, the United States' 2002 national security strategy (NSS) recognized the prevention of terrorism and regimes seeking nuclear, biological, and chemical weapons as the number one U.S. national security objective. It drew no distinction between terrorists who commit attacks and states that provide terrorist sanctuaries.[6] The NSS introduced a new use-of-force doctrine—an expanded concept of preemption. To ensure that a serious threat to the United States does not "gather," or grow over time, preemption permitted both an anticipatory use-of-force in the face of imminent attack, as well as a preventive use-of-force in the absence of evidence of an

---

2. Philip Zelikow, B. D. Jenkins, and E. R. May, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States (9/11 Report)* (Washington, D.C.: Government Printing Office, 2004), 263–264; Condoleezza Rice, *No Higher Honor: A Memoir of My Years in Washington* (New York: Crown, 2011).

3. George W. Bush, "Text of Bush's Speech at West Point," *New York Times*, June 1, 2002, http://www.nytimes.com/2002/06/01/international/02PTEX-WEB.html?pagewanted=all.

4. George W. Bush, "President Bush Outlines Iraqi Threat" (remarks by the President on Iraq, Cincinnati Museum Center-Cincinnati Union Terminal, Cincinnati, Ohio, October 7, 2002), https://georgewbush-whitehouse.archives.gov/news/releases/2002/10/20021007-8.html.

5. *National Strategy for Combating Terrorism* (Washington, D.C.: The White House, 2003), http://fas.org/irp/threat/ctstrategy.pdf; Aidan Hehir, "The Myth of the Failed State and the War on Terror: A Challenge to the Conventional Wisdom," *Journal of Intervention and Statebuilding* 1, no. 3 (2007): 307–332.

6. *The National Security Strategy of the United States of America* (Washington, D.C.: The White House, 2002), https://permanent.access.gpo.gov/lps90878/2002/nss.pdf.

imminent attack.[7] This new use-of-force doctrine was based on the premise that traditional rules of self-defense are not adequate to address non-state actor proliferation threats.[8] With the subsequent revelation of A. Q. Khan nuclear black markets, the United States faced the dismaying reality that there were many potential sources from which terrorists could buy what they wanted most: nuclear materials capable of making the next 9/11 even more deadly.[9]

The urgency of the threat posed by nuclear terrorism and the illicit trade of sensitive materials impelled the United States to call upon all United Nations (UN) member states to adopt a new antiproliferation resolution. In his address at the 58th UN General Assembly, President George W. Bush urged the UN Security Council to adopt a binding resolution with the objective of compelling states to refrain from all forms of state-sponsored WMD terrorism. President Bush encouraged all states to take necessary measures "to criminalize the WMD proliferation, to enact strict export controls consistent with international standards, and to secure any and all sensitive materials within their own borders."[10]

THE SECURITY COUNCIL SETS GLOBAL NONPROLIFERATION NORMS: LEGAL ANALYSIS

On April 28, 2004, the Security Council passed its most powerful counterproliferation instrument to date—Resolution 1540.[11] Enacted under Chapter VII binding powers,[12] Resolution 1540 mandated treaty-like obligations on all states to adopt and enforce effective laws to keep weapons of mass destruction, related materials, and technology out of the hands of terrorists. Resolution 1540 created legally binding obligations to close the gaps in the existing nonproliferation regimes within many of the traditional nonproliferation treaty instruments. One such gap was the nonuniversality of the system—in essence, states join nonproliferation treaties voluntarily, which lets countries of

---

7. Lawrence J. Korb, *A New National Security Strategy in an Age of Terrorists, Tyrants, and Weapons of Mass Destruction: Three Options Presented as Presidential Speeches*, No. 6 (Washington, D.C.: Council on Foreign Relations Press, 2003); Michael E. O'Hanlon, Susan E. Rice, and James Steinberg, *The New National Security Strategy and Preemption* (Washington, D.C.: Brookings Institution, 2002).

8. Jon Rosenwasser, "The Bush Administration's Doctrine of Preemption (and Prevention): When, How, Where?," Council on Foreign Relations, February 1, 2004, http://www.cfr.org/world/bush-administrations-doctrine-preemption-prevention-/p6799.

9. See, generally, Gordon Corera, *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the AQ Khan Network: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the AQ Khan Network* (Oxford: Oxford University Press, 2006).

10. George W. Bush, "President's Remarks at the United Nations General Assembly," September 12, 2002, https://georgewbush-whitehouse.archives.gov/news/releases/2002/09/20020912-1.html.

11. United Nations Security Council, Resolution 1540, April 28, 2004, http://www.un.org/press/en/2004/sc8076.doc.htm.

12. Chapter VII of the United Nations Charter sets out the UN Security Council's powers to maintain international peace and security. It allows the Council to "determine the existence of any threat to the peace, breach of the peace, or act of aggression" and to take military and nonmilitary action to "restore international peace and security." See "Charter of the United Nations," June 1945, accessed March 9, 2017, http://www.un.org/en/documents/charter/.

proliferation concern remain outside of nonproliferation rules.[13] Additionally, there was no multilateral legal regime placing limitations on private parties, including businesses or other non-state actors engaged in the manufacturing, possession, or transport of weapons-related technologies. The existing limitations on the international level targeted only states, not terrorists and illicit networks.[14]

Resolution 1540 established a range of far-reaching universal nonproliferation obligations. The first operative paragraph of the resolution requires states to refrain from taking any steps that could support non-state actors in acquiring, using, or transferring nuclear, chemical, or biological weapons and their delivery systems.[15] The first operative paragraph sends a strong political message to condemn and outlaw any type of state-sponsored WMD terrorism. It provides a normative requirement as a general precondition for implementing the more specific legal obligations that follow.

The second operative paragraph calls for criminalization of proliferation-related activities. It requires all member states to adopt effective domestic control and enforcement mechanisms over WMD materials and to criminalize possession, manufacturing, acquisition, development, transportation, transfer, or use of such materials.[16] The prohibition of nonproliferation activities also covers aiding, abetting, and financing thereof. This normative layer makes a clear reference to the special intent of nonproliferation activities for terrorism purposes, thereby recognizing the link between the threat of terrorism and non-state actor proliferation.[17]

The third operative paragraph of Resolution 1540 advances member states global nonproliferation obligations a step further. It requires member states address the illicit trafficking of WMD and WMD-related materials, commonly referred to as dual-use items. In doing so, member states are expected to establish and enforce four types of domestic measures and controls related to such materials: accounting and securing; physical protection; border and law enforcement, including

13. Suzette Grillot, ed., *Arms on the Market: Reducing the Risk of Proliferation in the Former Soviet Union* (New York: Routledge, 2013); Seema Gahlaut and Victor Zaborsky, "Do Export Control Regimes Have Members They Really Need?," *Comparative Strategy* 23, no. 1 (2004): 73–91; Richard T. Cupitt and Igor Khripunov, "New Strategies for the Nuclear Suppliers Group (NSG)," *Comparative Strategy* 16, no. 3 (1997): 305–315.

14. Masahiko Asada, "Security Council Resolution 1540 to Combat WMD Terrorism: Effectiveness and Legitimacy In International Legislation," *Journal of Conflict and Security Law* (2009); Jean Du Preez, "The 2005 NPT Review Conference: Can It Meet the Nuclear Challenge?," *Arms Control Today*, April 1, 2005, https://www.armscontrol.org/act/2005_04/duPreez.

15. United Nations Security Council, Resolution 1540, operative paragraph 1, explains that for the purposes of this resolution means of delivery are defined as "missiles, rockets and other unmanned systems capable of delivering nuclear, chemical, or biological weapons, that are specially designed for such use." Non-state actor is defined as an "individual or entity, not acting under the lawful authority of any State in conducting activities, which come within the scope of this resolution." Related materials are defined as "materials, equipment and technology covered by relevant multilateral treaties and arrangements, or included on national control lists, which could be used for the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery."

16. UN Security Council, Resolution 1540, operative paragraph 2.

17. Ibid.

combating illicit brokering and finance; and export, transit, and transshipment, including establishing end-user controls.[18]

The comprehensiveness and universality of Resolution 1540 obligations have distinguished it from other multilateral arms control treaties. For example, prior to Resolution 1540, multilateral arms control treaties and nonproliferation instruments traditionally did not require states to adopt transshipment or brokering controls. This was one of Resolution 1540's new features, along with its requirement that member states not simply pass domestic legislation, but also enforce it.[19] These clauses were widely regarded as the UN Security Council's attempts to close the loopholes of domestic export controls in response to revelations of A. Q. Khan's nuclear black markets, when corporate vendors exploited lax export controls in a number of countries to ship nuclear weapon designs and gas centrifuges to end users of proliferation.[20] Resolution 1540's goal was to close the weakest link in the nonproliferation chain by creating universal regulatory measures to thwart nuclear materials diversion into the illicit market.

Furthermore, Resolution 1540 called upon all member states to submit a national report identifying the steps that they have taken or intend to take to implement the resolution.[21]

RESOLUTION 1540 INSTITUTIONAL PLAYERS

To facilitate and monitor countries' domestic implementation, the UN Security Council also established an ad hoc subsidiary body—the 1540 committee,[22] consisting of all members of the Security Council.[23] The committee internally divides its activities into four working groups: monitoring and national implementation; assistance; cooperation with international organizations; and transparency and media outreach.[24] The committee has one rotating chair and three vice chairs.

Resolution 1540 authorized the 1540 committee to call upon outside expertise. A group of nine independent governmental experts was formed to assist the committee in its work (1540 group of experts).[25] The role of the 1540 experts is to examine each state's implementation of the resolution by analyzing national reports. The Security Council also recognized that some states may lack the

18. Ibid., operative paragraph 3.

19. Olivia Bosch, "A Legislative Evolution: Security Council Resolution 1540 Revisited," in *The Security Council as Global Legislator*, ed. Vesselin Popovski and Trudy Fraser (New York: Routledge, 2014), 102–108.

20. For more information on the A. Q. Khan nuclear smuggling network, see, for example, Sharon Squassoni, "Closing Pandora's Box: Pakistan's Role in Nuclear Proliferation," *Arms Control Today* 34, no. 3 (2004): 8–13.

21. UN Security Council, Resolution 1540, operative paragraph 4.

22. Ibid.

23. The committee was established under Rule 28 of the UN Security Council, "Provisional Rules of Procedure," available http://www.un.org/ar/sc/pdf/rules.pdf.

24. Briefing by the chairman of the Security Council committee established pursuant to UN Security Council, Resolution 1540, February 21, 2006.

25. Resolution 1540 experts are special consultants nominated to serve on the 1540 committee for up to five years. Each country can nominate one or more candidates. The 1540 committee scrutinizes the candidates, and the Secretary-General appoints the experts after consultations with the committee members.

capacity and resources to implement the resolution and invited states in a position to do so to offer assistance, in response to specific requests, to the states lacking the infrastructure, experience, or resources.[26]

The 1540 committee's work is further supported through the UN Secretariat. The UN Office of Disarmament Affairs (UNODA) provides material and logistical support to the committee. The UNODA advances the implementation of the resolution through its work with regional and international organizations, states, civil society, and industry representatives.

In summary, the 1540 committee, its group of experts, and the UNODA are the key institutional players that are responsible for facilitating Resolution 1540 implementation on the UN level.

A QUEST FOR LEGITIMACY: THE PROBLEM OF CONSENT

Resolution 1540 sparked controversy by breaking new ground in several ways. First, it dealt with dramatically different aspects of weapon proliferation including, but not limited to, regulating dual-use materials and technology, delivery means, as well as issues related to transshipment and physical security. Second, it mandated that all UN member states take action domestically, without each country giving its explicit consent.[27] Third, 1540 had all the characteristics of a general disarmament treaty, but it was not decided collectively. Rather than follow the traditional treaty-making precedent, the Security Council's permanent five members (P5) spent months in negotiations deliberating over the possible ways in which the Security Council could respond to a threat that the traditional arms control treaty regimes had been unable to address adequately and then developed a draft text of the resolution before it was handed to the nonpermanent members of the Security Council at the time.[28] In the end, the 15 members of the Security Council approved a document that created legally binding commitments for the rest of the international community.

Because Resolution 1540 created general legal obligations for all 193 UN member states without their explicit consent and without traditional treaty-making negotiation processes, it triggered criticism from many states. Two main arguments captured member states' frustration with the Security Council's action: procedural and substantive.

From a procedural point of view, many UN member states, especially in the Global South, criticized the Security Council for extending its mandate to conventional law, making and acting as a "world legislature." They argued that the council had entered into a new legislative phase,[29]

26. UN Security Council, Resolution 1540, operative paragraph 7.

27. Interview with Resolution 1540 expert, interviewee #9, New York City, October 16, 2013.

28. The permanent five members of the UN Security Council are China, France, Russia, the United Kingdom, and the United States. The 10 nonpermanent members, each serving two years, of the UN Security Council in 2004 were Algeria (2005), Angola (2004), Benin (2005), Brazil (2005), Chile (2004), Germany (2004), Romania (2005), Pakistan (2004), Philippines (2005), and Spain (2004).

29. In fact, the UN Security Council's first attempt utilizing Chapter VII to impose obligations of a legislative nature was Resolution 1373, "Counter-Terrorism," 2001. Resolution 1373 was passed 17 days after the 9/11 terrorist attacks and in many respects it mirrored the provisions of the 1999 Convention for the Suppression of the Financing of Terrorism

because from 1945 to 2001, the council's previous Chapter VII decisions were limited to: (1) responding to a concrete political or humanitarian crisis, hence the council's approach has been reactive as opposed to being proactive;[30] (2) enforcing existing international law;[31] (3) country specific;[32] (4) temporary in their nature;[33] and (5) reflecting council's actions on an ad hoc basis within the context of the threat occurring in a specific country and with no attempt to address functional threats to international peace and security.[34] A number of academics, diplomats, and policymakers have questioned the legitimacy of Resolution 1540 and the lack of deliberative democracy within the Security Council's decisionmaking process, arguing that a small number of states have formulated rules for the whole world and that Resolution 1540 is a form of hegemonic law and an encroachment on states' internal affairs without their explicit consent.[35]

Apart from the procedural issues, a second set of issues is substantive, touching upon the key concepts in nuclear disarmament. A number of states expressed frustration over what they perceived to be a lack of balance between nonproliferation and disarmament in Resolution 1540.[36]

---

without defining key notions, such as "terrorists," "terrorism," "international terrorism," or "terrorists acts." See, for example, Matthew Happold, "Security Council Resolution 1373 and the Constitution of the United Nations," *Leiden Journal of International Law* 16, no. 3 (2003): 593–610. Resolution 1373 begins by referring to the 9/11 attacks and by "reconfirming that such acts, like any act of international terrorism constitute a threat to international peace and security." The opening paragraph laid the legal ground for the Security Council's actions in accordance with Article 39 of the UN Charter. On the contrary, there was no such clear "imminent" threat to refer to for justifying the passage of Resolution 1540. See, for example, Daniel Joyner, *International Law and the Proliferation of Weapons of Mass Destruction* (Oxford: Oxford University Press, 2009), 181. Joyner argues that the Security Council used the events of 9/11 as a "catalyst" and "backdrop" to establish a much broader and temporally indefinite legal mandate to address the topic of international terrorism. The context in which Resolution 1540 was passed lacks evidence for a specific situation of an imminent threat to international peace against which the Security Council was responding.

30. Happold, "Security Council Resolution 1373 and the Constitution of the United Nations."

31. For example, the Security Council reinforced the principles of the UN Charter in the case of the 1990 Iraqi invasion of Kuwait, and reinforced the 1948 Genocide Convention in the case of Rwanda. Also see Georges Abi-Saab, *The Changing Constitution of the United Nations* (London: British Institute of International and Comparative Law, 1997); and Michael Byers, ed., *The Role of Law in International Politics: Essays in International Relations and International Law* (Oxford: Oxford University Press on Demand, 2000).

32. Even when the Security Council imposed universal obligations upon the general UN membership, those obligations had to do with maintaining peace and security in discrete cases where that peace and security had been threatened by the actions of one or a handful of states. See Georg Nolte "The Limits of the Security Council's Powers and Its Functions in the International Legal Systems: Some Reflections," in Byers, *The Role of Law in International Politics*.

33. Paul C. Szasz, "The Security Council Starts Legislating," *American Journal of International Law* 96, no. 4 (2002): 901–905.

34. Joyner, *International Law and the Proliferation of Weapons of Mass Destruction*.

35. For example, India, Cuba, Mexico, Namibia, Algeria, Nepal, Indonesia, South Africa, Pakistan, Brazil, and Iran have questioned the legitimacy of Resolution 1540. See United Nations Security Council, "4950th meeting," UN Document S/PV.4950, April 2004, http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/1540%20SPV%204950.pdf and UN Document A/58/PV.30, October 2003, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/569/12/PDF/N0356912.pdf?OpenElement. For India's declarations, see UN Document S/PV.4772. June 2003, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/PV.4772.

36. Interview with former Resolution 1540 expert #9, New York City, October 16, 2013.

Many Non Aligned Movement (NAM) members argued that the resolution has framed the issue in the nonproliferation narrative, which gave a "legitimate cause" to nuclear proliferation and ignored the disarmament obligations of states with nuclear weapons. Countries maintained that countering non-state actor proliferation fails to address the core of the problem—unless Nuclear Weapons States disarm and dismantle those weapons, there is always a risk of nuclear terrorism. Many developing countries perceived non-state actor proliferation and terrorism to be a problem of the West and viewed Resolution 1540 as a mechanism for the United States' global war on terror. Many refused to commit scarce resources to fighting nuclear proliferation because they considered it a low-priority threat for much of the developing world. Resolution 1540 was seen as an instrument through which "the West is protecting the West at the expense of the rest."[37] It played into the North and South divide, being interpreted as a means of continuing technology denial to developing countries to the advantage of the wealthy industrialized North. Some referenced the perceived lack of progress by the Nuclear Weapons States on their nuclear disarmament obligations as a reason to question the resolution's legitimacy.

EFFORTS TO OVERCOME LEGITIMACY DEFICIT: EARLY STRATEGIC CHOICES

Internal Political Context

In the immediate aftermath of Resolution 1540's passage, the UN Security Council had the challenging task of overcoming states' skepticism and facilitating the resolution's implementation—an ambitious legal mandate facing complicated political circumstances. The Council and the 1540 committee had to shape their responsibilities while navigating an environment in which (1) many states disagreed with the remit and legality of the Council to mandate generic legislative measures; (2) some states, because of the grounds upon which the United States invaded Iraq, feared that Chapter VII could open up the possibility of resorting to the use of force and sanctions for alleged 1540 noncompliance;[38] (3) some states were apprehensive of the 1540 committee and its undefined functions and mandate;[39] (4) a number of states opposed the lack of balance between nonproliferation and disarmament in the resolution;[40] and (5) many small states maintained the

37. Interview with senior UNODA official #6, New York City, October 22, 2013.

38. There was a fear among many UN member states that the adoption of Resolution 1540 through Chapter VII opens up a possibility for the Security Council or a unilateral actor to use military force against a noncompliant state. The United States' military operations in Iraq for its alleged WMD program has colored states' perception of Resolution 1540 and its negotiations. See, generally, Marc Weller, *Iraq and the Use of Force in International Law* (Oxford: Oxford University Press, 2010); and Sean D Murphy, "Efforts to Address Iraqi Compliance with UN Weapons Inspections," *American Journal of International Law* 96, no. 4 (2002): 956–962.

39. S/PV.4950, 15, http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/1540%20SPV%204950.pdf.

40. See, for example, "Statement by Ambassador D. S. Kumalo of South Africa to the Security Council on Non-Proliferation of Weapons of Mass Destruction," Permanent Mission of South Africa to the United Nations, April 22, 2004, http://www.southafrica-newyork.net/pmun/speeches/sc_nonproliferation.htm.

resolution was inapplicable and irrelevant to them due to their other pressing national security and development priorities, as well as a lack of domestic nuclear capabilities.[41]

As a result of the controversy sparked by the resolution, the 1540 committee was under political pressure to overcome these sensitivities and generate enthusiasm toward Resolution 1540's mandate.[42] Therefore, the 1540 institutional players developed strategies to reduce legitimacy concerns.

In response to states' skepticism, the Security Council's 1540 committee had a measured start. Much of the initial effort focused on shaping the internal characteristics of the committee's mandate.[43] In its early days, the committee's work was mainly organizational and—as many 1540 experts describe—"very low key."[44] The Security Council had to first internally conceptualize its novel mission of preventing non-state actor WMD proliferation and then develop processes that would assist states to implement the resolution domestically. Content analysis of the internal and publicly available documents, as well as interview data, suggests that the committee exercised a large degree of self-restraint in its early days to ease states' perceptions of the committee being intrusive into countries' internal affairs. During the first mandate, the committee developed its rules of procedure, selected eight independent 1540 experts, took some limited efforts to encourage states to submit first national reports, and adopted its first program of work.

On August 13, 2004, the 1540 committee approved its terms of reference (TOR).[45] The TOR specified the modalities of the committee's mandate, including its composition, structure of meetings, and decisionmaking procedures.[46]

In recruiting its first 1540 experts, the 1540 committee made efforts to appoint candidates from countries that lacked vested interests in nuclear issues or expressed resistance to 1540 mandate. Through this strategy, the committee aspired to dissipate legitimacy concerns and create a sense of local ownership of the 1540 implementation process. For instance, Mexico, South Africa, India, and Pakistan were some of the most vocal critiques of the Security Council's legislative mandate during the resolution's inception, and they all had nationals selected to be part of the 1540 group of experts. The appointment of an Eritrean national, Dr. Berhanykun Andemicael, as coordinator of the group of experts was another manifestation of the committee's attempt to create an organizational buy-in not only from specific countries, but also regions with limited WMD relevance. Andemicael served as an African 1540 expert from 2005 to 2012 and as the coordinator for the

41. Interview with former Resolution 1540 expert #5, New York City, May 7, 2014.

42. Interview with Resolution 1540 expert #2, New York City, October 7, 2013.

43. "Promoting Support for UNSCR [UN Security Council Resolution] 1540 Voluntary Fund," Cable: 09STATE122725: a-WikiLeaks; interview with Resolution 1540 expert, New York City, October 21, 2013.

44. Interview with Resolution 1540 expert #2, New York City, October 7, 2013.

45. Olivia Bosch and Ham Peter Van, *Global Non-Proliferation and Counter-Terrorism: The Impact of UNSCR 1540* (Washington, DC.: Brookings Institution Press, 2007), 235–238.

46. Chairman of the Security Council, "Committee Established Pursuant to Resolution 1540 (2004)," letter addressed to the president of the Security Council, December 8, 2004, UN Document S/2004/958, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2004/958.

group of experts during the first three years of his tenure. His Eritrean nationality and geographic origin mattered. Eretria is a small African nonnuclear weapons state (NNWS) with membership in the NAM. Even though these strategies were neither official nor publicized, choosing an Eritrean to be the face of the 1540 group of experts was a strategic decision by which the committee was seeking to make the resolution appeal to the Global South states.[47]

Initially, the group of experts was largely preoccupied with figuring out how to examine incoming country reports. The start of this process was full of internal political tensions. When the committee started to receive the first national reports, it became evident that there was an enormous diversity in terms of content, structure, length, and quality of the reports. Some countries followed the structure of Resolution 1540, others reported what they believed was necessary. At that early stage, it was more about the quantity of responses rather than quality. To some extent, the completeness of the reports served as an indicator of states' attitudes toward Resolution 1540, and most continued to maintain a low opinion of the resolution and its requirements. Apart from the major developed states, which generally submitted substantial reports, a number of countries submitted reports that basically had no meaningful content other than confirmation that the submitting state lacked WMD capabilities.

There were disagreements between the committee and its experts over defining a process by which the experts could assess all country reports. The committee's original preference was to look into each country submission individually and report back with a country-specific assessment. Many of the experts disagreed with such a country-centric approach and proposed to develop a standardized evaluation tool. After a few months of internal discussions, the committee approved the Resolution 1540 matrix template.[48] This matrix has become the primary method used by the committee and the experts to organize and examine the information submitted by member states about their implementation of Resolution 1540.[49] The experts' job was to transfer national reports into 1540 matrices. Differences in opinion between the experts themselves existed as to what was considered acceptable, how responses should be categorized, and whether the experts could question the veracity of states responses. Much discussion ensued over the experts' actions once the national reports data were transferred into the matrices. There were many diplomatic exchanges about whether to follow a confidential assessment process supported by sanctions in the event of noncompliance or to introduce an inclusive and transparent process whereby the committee could reach out to states that submitted their reports to solicit additional

47. Interview with former Resolution 1540 expert #4, New York City, May 2, 2014.

48. A matrix is based on the provisions of the resolution and is used by the committee and the experts to store the information stemming out of the national reports. There are 300+ questions/fields in the matrix. See United Nations Security Council, "Letter dated 25 April 2006 from the Chairman of the Security Council Committee established pursuant to resolution 1540 (2004) addressed to the President of the Security Council," S/2006/257, April 2006, http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/WMD%20S%202006%20257.pdf. The matrices, however, are not an instrument to measure domestic compliance. Experts may use the information contained in matrices as a reference tool for channeling technical assistance to a member state.

49. Skype interview with Resolution 1540 expert #9, April 18, 2013.

information or seek clarification on the topics covered by the first reports.[50] Subsequently, facilitating 1540 implementation through dialogue and cooperation became the committee's most significant feature.

Turning Committee into Cooperative and Voluntary Tool

With a universal mandate backed by Chapter VII enforcement power, the 1540 committee was organized as a Special Political Mission under the Sanctions and Monitoring cluster.[51] This cluster usually consists of monitoring teams, panels, and other groups that bear the responsibilities of monitoring the implementation of Security Council resolutions and reporting on the sanctions imposed by the council.[52] The committee chose not to become a UN sanctions regime. Instead, from the very beginning, transparency and openness characterized the work of the committee.[53] Unlike the North Korea or Iran sanctions committees, the 1540 committee refrains from pursuing any investigative, monitoring, or sanctioning measures. It has taken this course because the committee lacked legitimacy and a good reception in the first place; and as a result, the UN member states would refuse to cooperate with any punitive measures for implementing 1540. Instead, the 1540 institutional players combined their efforts to diffuse the apprehensions about the resolution and incentivize states' domestic implementation. Cooperation and flexibility seemed the right strategy by which to engage with states. More specific efforts included marketing the resolution as a cooperative tool, raising awareness through outreach activities and bilateral dialogues, developing strategies that would preserve national discretion of states and not usurp national sovereignty,[54] and using rhetorical strategies for persuasion.[55]

Outreach and Marketing Activities

The idea to organize Resolution 1540 workshops with governments and/or regional and subregional organizations has emerged as a method to market the resolution to member states, most particularly to those that were originally hostile to it. One of the senior leaders at the UNODA came up with this concept of outreach workshops. From July 2006 to December 2007, the

---

50. United Nations Security Council, "Report of the Security Council by the Chairman of the Security Council Committee Established Pursuant to Resolution 1540 (2004)," S/2005/799, 17. http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/1540%20S2005%20799.pdf.

51. "Special Political Missions and other political initiatives," Second report of the Secretary-General, https://dpa-ps.atavist.com/spmreport_2014.

52. Ibid.

53. UN Security Council, "Report of the Committee Established Pursuant to Resolution 1540 (2004)," 2008; UN Security Council, "Report of the Committee Established Pursuant to Resolution 1540 (2004)," UN Document, S2008493, July 2008, http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Disarm%20S2008493.pdf.

54. Interview with former Resolution 1540 expert #6, May 26, 2014.

55. For instance, both the UNODA and the experts always use the word "voluntary" in regards to both substantive and procedural 1540 obligations. The common discourse is "voluntary" national reporting, "voluntary" national action plans, "voluntary" state visits. Furthermore, the experts always reiterate that the committee does not use matrices to measure member states' compliance with the resolution's requirements. Instead, matrices serve as a useful tool to identify gaps and channel technical assistance.

UNODA organized three inaugural, high-level regional workshops in Asia-Pacific hosted by China;[56] in Latin America and the Caribbean hosted by Peru;[57] and in Africa hosted by Ghana.[58] These workshops brought players together to raise awareness about the resolution's requirements and assure those states in the region (especially the NAM members) that the committee would not impose burdens on them.[59] Organizing and hosting similar workshops has become a cornerstone of the UNODA's support to Resolution 1540's implementation. In fact, up until 2011, when the 1540 committee conducted its first country-specific visit, both the group of experts and UNODA mainly maintained an advocacy role to raise awareness about the resolution.[60] In the inner circles, the delegates jokingly named the committee as a public relations committee, which speaks to the fact that most of the work pertinent to 1540 was information sharing.

Continued multilateral and bilateral dialogues between the 1540 key players and member states helped reshape states' attitudes toward the resolution. Member states realized that Resolution 1540 was voluntary and that their fears that the UN Security Council would become a world legislator did not materialize. The committee does not impose measures on states regarding non-state actor WMD proliferation. Rather, it tries to use the resolution as a basis for countries to take the necessary measures in their domestic structures. It helps states to push the agenda of introducing 1540-related regulatory and enforcement measures within their national jurisdictions.[61] To place all non-P5 Security Council members on equal footing with their P5 counterparts and give them a sense of collegiality, the 1540 committee relied on consensus decisionmaking. Some non-P5 committee members highly value the participatory environment of the committee's work, as—unlike the North Korea and Iran sanctions committees—they are encouraged to participate in 1540 activities, recommend decisions to the Security Council, or block anything from the committee's agenda.[62]

Keeping National Sovereignty through Imprecise Obligations: "What to Do, but Not How to Do"

Most of the Resolution 1540 obligations were kept vague and general. The resolution did not fully spell out how to interpret the myriad 1540 obligations and what constitutes compliance. Many have argued that the resolutions tells *what* to do, but not *how* to do. Such imprecision was

---

56. UN Department of Disarmament Affairs, "United Nations Seminar on Implementing UN Security Council Resolution 1540 in Asia and the Pacific," 11 DDA Occasional Papers, October 2006, http://www.un.org/disarmament/WMD/1540/pdf/OP11-Asia_Pacific.pdf.

57. UN Department of Disarmament Affairs, "United Nations Seminar on Implementing UN Security Council Resolution 1540 in Latin America and the Caribbean," 13 DDA Occasional Papers, December 2007, http://www.un.org/disarmament/WMD/1540/pdf/OP-13-Latin_America.pdf.

58. UN Department of Disarmament Affairs, "United Nations Seminar on Implementing UN Security Council Resolution 1540 in Africa," 12 DDA Occasional Papers, May 2007, http://www.un.org/disarmament/WMD/1540/pdf/OP12-Africa.pdf.

59. Interview with former Resolution 1540 expert #7, New York City, April 28, 2014.

60. Ibid.

61. Interview with Resolution 1540 committee member (state representative) #2, New York City, May 2, 2014.

62. Interview with Resolution 1540 committee member (state representative) #3, New York City, May 1, 2014.

deliberate. The Security Council intentionally left methods of implementation up to the discretion of individual governments. This was a tactic to mitigate member states' resistance toward Resolution 1540 on the grounds that the Security Council was usurping the sovereignty of states. The generic language was meant to reinforce the fact that one size does not and will not fit all. The implementation depends on national discretion and on what states devise as appropriate and effective policies. Some states face more favorable conditions for implementation of the resolution than others. "What to do, but not how to do" served as a slogan for the 1540 key players to signal to countries that the 1540 committee is not a world policeman, and that states preserve their national sovereignty in deciding how to implement their 1540 obligations in accordance with their national priorities.

The Passage of Time: Changing Terrorist Threat Perceptions and States' Attitudes

Facilitating Resolution 1540's implementation through dialogue and cooperation has become the 1540 committee's key characteristic. Cooperative and outreach activities have served the UN Security Council's political priority to reverse states' negative perceptions toward the resolution, resulting in 176 national implementation country reports submitted to the committee. Furthermore, the passage of time and growing terrorist threats have also helped many states appreciate the importance of fighting WMD terrorism.[63] After 9/11, terrorist attacks did not decrease. Quite the contrary—over the past 15 years the number of terrorist incidents has grown, the targeting policies of terrorist groups have dramatically changed, illicit trafficking of WMD materials has continued to occur, and the networks of terror and criminality have expanded their global reach and capabilities.[64]

After the eruption of the Syrian war in 2011, the threat of WMD terrorism has become more real. The Organization for the Prohibition of Chemical Weapons (OPCW) has confirmed the use of toxic chemicals, including the nerve agent sarin or sarin-like gas during the Syrian conflict. There is a risk that insurgent and terrorist groups could have access to WMD stockpiles.[65] The U.S. intelligence community estimates that both the Assad regime and non-state actors (i.e., Islamic State of Iraq and Syria [ISIS]) have used chemicals during the war.[66]

---

63. Interview with UNODA senior official #4, New York City, October 24, 2013.

64. More than 61,000 terrorism incidents have been recorded from 2000 to 2014 according to the Institute for Economics and Peace. See Global Terrorism Index 2015: Measuring and Understanding the Impact of Terrorism, Institute for Economics and Peace, November 2015, http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf. Erin Miller, Background Report: Mass-Fatality, Coordinated Attacks Worldwide, and Terrorism in France (2015), National Consortium for the Study of Terrorism and Responses to Terrorism, November 16, 2015, https://www.start.umd.edu/pubs/START_ParisMassCasualtyCoordinatedAttack_Nov2015.pdf.

65. David M Luna, "Neutralizing Radicalized Threat Networks, Disrupting WMD Illicit Traffickers and Targeting Corrupt Facilitators," in *Nuclear Threats and Security Challenges* edited by Samuel Apikyan and David Diamond (Dordrecht: Springer Netherlands, 2015), 13–22.

66. James R. Clapper, "Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence," February 9, 2016, http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

In addition to incidents in Syria, in June 2011, Moldovan authorities detained a group of middlemen who attempted to sell 4.4 grams of highly enriched uranium (HEU) in a cylindrical lead container to an undercover police agent.[67] In October 2013, Russian authorities prevented Islamist militants from planting a bomb at the Maradykovsky chemical weapons storage and disposal facility in the Kirov region.[68] After the March 2016 Brussels attacks and revelations of ISIS militants' spying on a Belgian nuclear scientist, there has been speculation that ISIS is trying to get its hands on nuclear materials for a dirty bomb.

As terrorism incidents continued to grow and expand, many developing states started to realize that terrorism no longer concerns only Western countries. Attacks may occur in both developed and developing countries, but developing countries suffer harsher consequences due to their weak domestic preparedness and limited resources.[69] For example, during the 2008 Mumbai attack, the death toll increased because the local police lacked training and the ability to cordon off the attack sites, and national security guards along with other forces responded extremely slowly. There was a lack of coordination between municipal firemen and local police, the strategic communication was poorly managed, and hostage rescue plans had severe defects.[70]

The interpretation of what constitutes Resolution 1540 obligations has been refined over time. A number of countries started to realize that the resolution is not exclusively about securing WMD materials, but could also help improve public health, fight illicit trafficking of small arms and light weapons (SALWs), and secure domestic borders—security problems that are relevant for the Global South. Developing countries saw a dual-use purpose in complying with the requirements of this counterproliferation instrument. For example, emergency response teams use the same communication systems irrespective of whether they are managing a natural or WMD disaster. Resolution 1540 provides an opportunity to further both security and development, because it offers a possibility for poorer countries to tap on the resolution's security-related assistance program to simultaneously meet many of their development and capacity-building objectives.[71] A properly trained police is necessary to prosecute the illicit trade, transfer, or transshipment of both WMD materials and SALWs. Likewise, a similar set of resources and capabilities is necessary to prevent both human trafficking and nuclear proliferation. This flexibility and the ability to adjust 1540 obligations to

---

67. "Six People Arrested in Moldova over Bomb-Grade Uranium," *Telegraph,* June 29, 2011, http://www.telegraph.co.uk/news/worldnews/europe/moldova/8607235/Six-people-arrested-in-Moldova-over-bomb-grade-uranium.html.

68. "ICT's Incidents Database Periodical Report: Summary of Terrorist Incidents and Counter-Terrorist Operations Worldwide," October 2013, https://www.ict.org.il/UserFiles/Database%20Report%20October%202013.pdf.

69. Interview with UNODA senior official # 4, New York City, October 24, 2013.

70. Angel Rabasa et al., *The Lessons of Mumbai* (Santa Monica, CA: RAND, 2009), http://www.rand.org/pubs/occasional_papers/OP249.html; Padma Rao Sundarji, "India's Lack of Preparedness Raised Mumbai Death Toll," *McClatchy DC*, December 3, 2008, http://www.mcclatchydc.com/news/nation-world/world/article24513016.html. Terrorists have exploited a target country's state of preparedness in other attacks too. For instance, a poor communication and coordination between policy and military combined with the presence of multiple plainclothes law enforcement first respondents caused confusion in the Al Shabaab's September 2013 attack at the Westgate mall in Kenya.

71. Brian D. Finlay, "Bridging the Security/Development Divide with UN Security Council Resolution 1540: A Case Study Approach" (Washington, D.C.: Stimson Centre, 2009).

serve countries' local needs and national interests made Resolution 1540 more attractive to domestic stakeholders, especially in the Global South.

Unprecedented Political Consensus

The 1540 committee's efforts to build legitimacy have created a strong political consensus among UN member states for supporting the resolution's goals. At the time of this writing, 176 countries have submitted a national compliance report at least once;[72] at least 24 states have developed national action plans outlining their national priorities for implementing 1540 obligations;[73] on average, countries have reported taking around 145 domestic measures to comply with the resolution;[74] and the 1540 committee's group of experts have conducted at least 14 country visits.

Given states' early apprehensions over UN Security Council's reference to its Chapter VII powers in the adoption of Resolution 1540, the high level of reporting is indeed remarkable. Some suggest that it serves as a metric to indicate an amplified worldwide commitment to 1540 goals. The 1540 committee's original two-year mandate was extended twice—in 2006 and 2008. In April 2011, the Security Council unanimously extended the UN Security Council's Resolution 1540 mandate for another 10 years through 2021.[75] Once seen as interference by the Security Council in domestic matters, Resolution 1540 is now viewed as states coming together for a common cause.[76] Perceptions have shifted dramatically since its inception.

The Flexible Mandate

The voluntary nature of the 1540 committee's work has created unprecedented political consensus for Resolution 1540. Meanwhile, this structure posed some limits on the committee's ability to effectively guide and support domestic implementation. For many years, the committee's number one priority has been securing universal reporting. The high number of reports indicates broad commitment to the 1540 goals, but these numbers produce a false sense of confidence in 1540's universal implementation and the capacity of states to deal with radiological or nuclear terrorism. Oftentimes, these reports reference outdated and non-WMD–related regulations or even contain false information (e.g., the Syrian report to the 1540 committee noted that Syria does not possess chemical weapons). The 1540 group of experts do not conduct critical analysis of national reports or carry out threat assessment and country profiling. Therefore, country reports on implementation are an insufficient metric of the resolution's success.

---

72. Review of the Implementation of Resolution 1540 (2004) for 2015, S/2015/1052, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2015/1052.

73. United Nations 1540 Committee, National Implementation Plans, http://www.un.org/en/sc/1540/national-implementation/national-implementation-plans.shtml.

74. *Supra note* 72, United Nations Security Council. Letter from the Chair of the Security Council Committee, December 2015, S/2015/1052 http://undocs.org/en/S/2015/1052.

75. UN Security Council, Resolution 1810, April 2008, http://unscr.com/en/resolutions/doc/1810.

76. UN Security Council, "What Was Once Seen as Security Council Interference in Domestic Affairs Now Viewed as States 'Coming Together for Common Cause', 1540 Review Hears Upon Closing," UN Document SC/9754, September 30, 2009, http://www.un.org/press/en/2009/sc9754.doc.htm.

The 1540 committee is still struggling to institutionalize the assistance mechanism. Thus far, the capacity-building efforts have been limited to workshops, seminars, and trainings. At the time of this writing, the committee has not channeled any financial or technological 1540-led assistance to countries that need help (e.g., assisting radiation detection efforts in ports handling massive amount of container traffic). Many criticize the assistance mechanism, arguing that the committee is essentially serving as a post office that mainly circulates member states' assistance requests to assistance providers.

CONCLUSION

The key characteristic of the 1540 committee is its flexible and cooperative nature. In defining its mandate, the committee chose not to become a UN sanctions regime, either in the name of nonproliferation or counterterrorism. It worked transparently, engaged in dialogue with the UN member states, exercised self-restraint, and marketed the UN Security Council's Resolution 1540 through outreach activities. While these early strategic choices triggered a more positive outlook on the resolution, many of the committee's practices reflected a search for legitimacy rather than efficient implementation of Resolution 1540's goals. There were constant attempts to diffuse member states' fears in order to gain acceptance for the resolution's implementation. The voluntary nature of the committee's work has created strong political consensus for supporting the resolution, but it has restricted the committee's ability to conduct critical analysis of country reports, carry out country profiling, and meaningfully work with countries of proliferation concern. In the past 10 years, the 1540 regime has been successful in overcoming its legitimacy crisis. The most vocal critics of the resolution turned into its most enthusiastic supporters. Despite this progress, much remains to be done in order to achieve the original goals of the resolution. In 2011, the 1540 committee's mandate was extended for 10 more years. In its second decade, the regime will no longer have the initial legitimacy challenges and, therefore, the focus should be on improving the effectiveness of its implementation.

After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities

Alexandra Van Dine[1]

The Stuxnet virus set off alarm bells all over the world when it was discovered in 2010. Many observers viewed this unprecedented cyber attack on a nuclear facility as the dawn of the age of cyber war—"the keystroke heard 'round the world."

Stuxnet also had significant implications for nuclear security. The attack revealed a troubling reality: in the future, cyber weapons could be used against nuclear facilities to achieve consequences far more serious than those observed at the Natanz uranium enrichment facility in Iran.

Terrorist groups have stated their desire to acquire weapons of mass destruction. Cyber weapons provide a new attack vector for groups determined to achieve this goal. Security and surveillance systems can be hacked to mask the theft of weapons-usable nuclear materials, or vital control systems can be compromised, potentially leading to a serious radiological release. Given repeated recent discoveries of malware—targeted or otherwise—at nuclear facilities, it is not impossible that malicious actors could gain access to these systems.

Stuxnet was an extremely precise weapon deployed against a highly secure facility for a very limited purpose. At no point were human lives or the environment in danger. However, this will not always be the case. With the code for Stuxnet now widely available online, it may only be a matter of time before a group intending to cause harm deploys a less discriminate weapon against a less secure, higher-consequence target like a nuclear power plant or nuclear materials storage facility.

The international community must learn from Stuxnet's lessons to prevent such an outcome.

---

1. Alexandra Van Dine is a program associate with the scientific and technical affairs team at the Nuclear Threat Initiative (NTI), where she works on cyber security-related projects and the NTI Nuclear Security Index. She is a graduate of Georgetown University's Edmund A. Walsh School of Foreign Service. The views presented in this paper are the author's alone and do not necessarily reflect those of the Nuclear Threat Initiative.

INTRODUCTION

Throughout late 2009 and 2010, centrifuges spinning in Iran's Natanz uranium enrichment facility started to break at unusually high rates. In time, it would become clear that these disruptions were not standard mechanical failures; they were the result of Stuxnet, a cyber weapon designed and deployed with the goal of slowing or halting Iranian uranium enrichment.

Stuxnet is a computer worm, that is, a virus with the ability to copy itself and travel quickly between computers. It was crafted to quietly take over industrial control systems and break the fragile, antiquated IR-1 centrifuges spinning at Natanz. Natanz's technology is widely viewed by the international community to be critical to Iran's pursuit of nuclear weapons.

Revelations about Stuxnet opened eyes in countries all over the globe. This was the first instance of a targeted cyber attack causing physical damage to highly sensitive infrastructure. Many observers viewed this discovery as "the keystroke heard 'round the world"—effectively, the dawn of the age of cyber warfare. Examining Stuxnet in a larger context, however, also reveals a troubling gap in the advancements made in nuclear security over the past decade. Nuclear facilities around the world remain too vulnerable to cyber attacks that could facilitate the theft of nuclear material or a radiological release.

Stuxnet, the code for which is now available to anyone with Internet access and sufficient funds, was able to penetrate a highly secure facility and cause physical damage intended to be limited in scope. But what if an adversary instead sought more destructive consequences?

Despite Stuxnet's warnings, the world is still playing catch-up when it comes to the cyber dimension of nuclear security. This paper will evaluate the current threat and approach to cyber security at nuclear facilities, discuss the Stuxnet case and its implications, and make recommendations based on the Stuxnet case for strengthening cyber-nuclear security.

THE THREAT

Leaders around the world have rightly expressed concern about the adequacy of physical security at nuclear facilities in the face of terrorist threats. As a result, countries have taken important steps to strengthen nuclear security domestically, and many international organizations—the International Atomic Energy Agency (IAEA), the World Institute for Nuclear Security (WINS), the United Nations, and Nuclear Security Summits, to name a few—have undertaken efforts to improve international preparation, prevention, and response.

The vast majority of this work has focused on key issues like the insider threat, physical security measures, and materials control and accounting technologies and procedures. Progress in these areas is a critical precursor to a more secure world and must benefit from continued investments of money, time, and attention. However, these efforts, important as they are, have been undertaken without sufficient attention to the cyber threat to nuclear security. In order to achieve the highest levels of global nuclear security, international efforts must also address the cyber threat and its implications for nuclear facilities.

Cyber attacks can have effects on par with a safety incident or physical security breach. For example, an adversary could hack into alarm or surveillance systems and disable them, masking the actions of malicious intruders. Materials control and accounting systems could be hacked in order to hide the theft of nuclear materials. In a worst-case scenario, an attacker could tamper with vital reactor control systems, potentially leading to radiological release with serious off-site consequences.

Recent decades have seen a proliferation of digital technologies across the nuclear enterprise. These technologies have real benefits in terms of safety and physical security; however, they do create cyber vulnerabilities that often go unanalyzed or even unnoticed. More digitization means more exploitable weaknesses, thus creating a dynamic and pervasive threat that strains national and international authorities alike.

Moreover, terrorist organizations like al Qaeda and the Islamic State of Iraq and the Levant (ISIL) are seeking radiological and nuclear capabilities and place a premium on attacks that maximize panic and destruction.[2] Cyber vulnerabilities could be leveraged in pursuit of these goals.

CURRENT STATUS

Government authorities, national regulators, nuclear industry, and international organizations have recognized the cyber threat to nuclear facilities and are taking some steps to develop and implement solutions. In the United States, for example, the Nuclear Regulatory Commission (NRC) and Department of Homeland Security (DHS) have defined roles in preventing and responding to a possible cyber attack at a nuclear facility. International organizations have also embraced their role, with the IAEA in particular working hard to provide training opportunities to regulators and facility staff around the world, develop and circulate guidance, and facilitate international dialogue on the topic. The nuclear industry has also been a leader in this area, with the Nuclear Industry Summit convening an international working group of industry representatives to consider the threat, develop solutions, and bring high-level attention to cyber security. The fact that this group will continue meeting, even in the absence of continued Nuclear Security Summits, demonstrates the industry's commitment to mitigating this threat.

Although all these efforts are useful and necessary to improving global cyber-nuclear security, the world remains underprepared to meet this dynamic threat. The current approach is unable to move as quickly and flexibly as the cyber threat and is unevenly applied geographically. Too many countries with nuclear materials or high-consequence nuclear facilities lack appropriate legal and regulatory frameworks in this area. What limited human capacity that exists at the nexus of cyber and nuclear security is heavily concentrated in North America, Europe, and Russia, meaning that many countries with new or expanding nuclear programs lack necessary technical expertise. Finally, cyber-security strategies tend to rely on technological measures like air gaps, firewalls, and

2. See Rolf Mowatt-Larssen, "Al Qaeda's Nuclear Ambitions," *Foreign Policy*, November 16, 2010, http://foreignpolicy.com/2010/11/16/al-qaedas-nuclear-ambitions/ and Kim Sengupta, "ISIS [Islamic State of Iraq and Syria] Nuclear Attack in Europe Is a Real Threat, Say Experts," *Independent*, June 7, 2016.

antivirus tools that have been proven fallible to the exclusion of other, perhaps more effective measures.

Lack of Legal Frameworks

Moreover, data exists that suggests a global lack of preparedness. The 2016 NTI Nuclear Security Index, a first-of-its-kind ranking of nuclear security conditions around the world, asked four basic questions about cyber security at nuclear facilities in countries with one kilogram or more of weapons-usable nuclear material or high-consequence nuclear facilities:[3]

1. Does the country require nuclear facilities to be protected from cyberattack?
2. Does the country require nuclear facilities to identify critical digital assets?
3. Does the country incorporate cyber threats into its design basis threat or other threat assessment?
4. Does the country require performance-based testing of its cyber security measures?

Scoring was based on publicly available laws and regulations, and did not measure implementation. Therefore, a high score does not necessarily guarantee security, although it does provide some idea of how seriously countries are taking the cyber threat. Key results included:

- Of 24 countries with weapons-usable nuclear materials, only 9 countries scored a maximum score on cyber security. Seven scored zero.
- Of 23 countries with high-consequence nuclear facilities, only 4 countries earned a maximum score. Thirteen scored zero, including some that are considering expanding their use of nuclear power or beginning new programs.
- In total, of 47 countries with weapons-usable nuclear materials or high-consequence facilities, 20—nearly half—scored a zero on cyber security.

These results suggest that the existence of key laws and regulations related to cyber security at nuclear facilities is disturbingly uneven. This threat is global—a cyber attack that causes damage at a nuclear facility could have consequences that reverberate around the world. Therefore, it is troubling that so many countries are not taking basic regulatory steps to protect nuclear infrastructure from attack.

Limited Human Capacity

Even where countries are working to improve their regulatory frameworks and operational processes and procedures, it is not always possible given the uneven distribution of limited human capacity in the cyber-nuclear space. Practitioners must possess a knowledge of digital control systems in nuclear environments, a skill set that is increasingly rare. There have been few of these experts; now, many have retired, and a limited number of candidates are entering the field. Those who remain tend to be concentrated in just a few countries. This leaves many countries developing or expanding nuclear energy programs grasping for solutions. As long as so few experts are concentrated in so few places, solutions will be difficult to devise and implement.

3. For more information about the NTI Nuclear Security Index, see www.ntiindex.org.

Overreliance on Technologies

The current operational approach to cyber security at nuclear facilities also tends to overestimate the effectiveness of certain technological measures. Defense strategies tend to be premised on the assumption that it is possible to completely prevent cyber attacks. Accordingly, they rely heavily on measures like air gaps, firewalls, and antivirus tools to deny access to attackers. Unfortunately, several cases in the past few years have demonstrated that these measures are not fully effective. These include discoveries of malware designed to provide remote access to adversaries and seek out login credentials at a German power plant; malware found in a Japanese nuclear power plant and a facility that handles plutonium and other nuclear materials; and a hack and subsequent data release affecting Korea Hydro and Nuclear Power, South Korea's nuclear operator.[4]

Although these tools can and do play an important role in cyber security, it is not reasonable to expect them to hold up to sustained attacks from determined adversaries. Such adversaries think creatively, move quickly and flexibly, leverage the full suite of system capabilities, and take advantage of enduring vulnerabilities that cannot be patched, such as inherent human imperfection. Therefore, a truly effective cyber-security strategy cannot be based upon prevention alone, and is ill-served by focusing on fallible technological measures to the exclusion of other security practices and solutions.

STUXNET: AN OVERVIEW

The cyber operation against Natanz leveraged two versions of the Stuxnet virus, the first more intensive and complicated than the second. The first part of the attack targeted the systems that protected the centrifuges spinning at the Natanz uranium enrichment plant. The malware tried to overpressurize the centrifuges by directly impacting the very system meant to prevent this from happening. At Natanz, this system was particularly elaborate due to the equipment it was protecting—outdated and unpredictable IR-1 centrifuges. Without such a system to compensate for the antiquated technology, the centrifuges would be too unpredictable to use.[5]

The IR-1 was selected for use at Natanz because Iran could produce the model at massive scale, which meant that frequent breakage was acceptable. IR-1 centrifuges only tend to work reliably if their parts are fabricated with incredible precision and they are operated in an environment with

---

4. For more on Germany, see Christoph Steitz and Eric Auchard, "German Nuclear Power Plant Infected with Computer Viruses, Operator Says," Reuters, April 26, 2016, http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS. For more on Japan, see "Monju Power Plant Facility PC Infected with Virus," *Japan Today*, January 7, 2014, http://www.japantoday.com/category/national/view/monju-power-plant-facility-pc-infected-with-virus; and "Nuclear Center Waits Over a Year to Report Cyber-Attack," *Asahi Shimbun*, May 19, 2016, http://www.asahi.com/ajw/articles/AJ201605190028.html. For more on South Korea, see Meeyoung Cho and Jack Kim, "South Korea Nuclear Plant Operator Says Hacked, Raising Alarm," Reuters, December 22, 2014, http://www.reuters.com/article/us-southkorea-nuclear-idUSKBN0K008E20141222.

5. Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, November 19, 2013, https://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.

specific equipment. Iran could not create those conditions, and therefore had to lower the operating pressure of their centrifuges in order to decrease the stress on the sensitive rotors. This meant that fewer centrifuges would go offline as a result of damaged rotors, but that efficiency would decrease due to the lower operating pressure.[6] In order to compensate for this inefficiency and frequent centrifuge failure, Iranian scientists constructed a cascade protection system that ensured continuation of enrichment, even when one or more centrifuges broke.[7] At Natanz, a cascade was a grouping of 164 centrifuges connected together by pipes. Uranium gas would flow through those pipes and into the centrifuges in stages; each stage enriched the gas further, separating out isotopes needed for nuclear reaction and concentrating them in the gas.[8]

Using valves installed on each centrifuge, the system could isolate a troublesome centrifuge from the rest of the cascade long enough for an engineer to replace it while the process continued across the rest of the cascade. However, sometimes shut-offs occurred faster than engineers could fix them, leading to multiple isolated centrifuges within the same stage and a resultant rise in operating pressure, which is not good for the smooth operation of centrifuge cascades.[9]

To address this flaw, the Iranians installed exhaust valves at each stage to relieve this pressure. When pressure, as monitored by a sensor, exceeded a certain threshold, the exhaust valve would open and release extra pressure. These sensors and valves were operated by Siemens S7-417 industrial controllers that were tiny computer systems connected directly to the equipment.[10] Although this somewhat convoluted solution did keep the centrifuges up and running, it greatly increased the complexity of digital systems at Natanz. This provided fertile ground for Stuxnet's creators, who developed an attack that industrial control systems expert Ralph Langner described as "so far out, it leads one to wonder whether its creators might have been on drugs."[11]

One of the first steps of the Stuxnet attack was camouflage; that is, the malware was designed to mask its own activities when the attack executed, usually about once each month. Immediately before an attack, the malware would record exactly 21 seconds of the normal values displayed on the sensors protecting the cascades.[12] Then, Stuxnet would replay those 21 seconds in a constant loop as the attack took place, thus effectively projecting normalcy to facility operators while masking the weapon's activities from any network surveillance or monitoring capabilities.[13]

---

6. Ibid.

7. "Basic Attack Strategy of Stuxnet 0.5 Rev. 1," Institute for Science and International Security [ISIS], February 28, 2013, http://isis-online.org/isis-reports/detail/basic-attack-strategy-of-stuxnet-0.5/.

8. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

9. "Basic Attack Strategy of Stuxnet 0.5 Rev. 1."

10. Dan Goodin, "Revealed: Stuxnet 'Beta's' Devious Alternate Attack on Iran Nuke Program," *Ars Technica*, February 26, 2013, http://arstechnica.com/security/2013/02/new-version-of-stuxnet-sheds-light-on-iran-targeting-cyberweapon/2/.

11. Langner, "Stuxnet's Secret Twin."

12. Ibid.

13. Joby Warrick, "Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyber Attack," *Washington Post*, February 15, 2011, https://www.washingtonpost.com/world/irans-natanz-nuclear-facility-recovered-quickly-from-stuxnet-cyber-attack/2011/02/15/ABUIkoQ_story.html.

Safely hidden from view, the malware would close the valves that isolated centrifuges in such a way that pressure was raised on the rest of the centrifuges in a given cascade. This, in turn, placed greater stress on the rotor, ultimately breaking the centrifuge.[14] This would go on until the attacker decided that a sufficient number of centrifuges had been damaged, and conveyed the appropriate message to the virus via a complex command-and-control system.[15] Destroying too many centrifuges at once would have been easily detected by Iranian engineers and the true cause of the damages discovered much faster.[16]

At some point in 2009, the attacker changed course and deployed a second version of Stuxnet. This time, the malware targeted a different component: Siemens 315 programmable logic controllers (PLCs) that controlled centrifuge frequency converters, which are responsible for determining rotor speed. This was a much easier attack, and the methods by which the malware achieved it were far more direct than those of the first Stuxnet version.[17]

Unlike the first stage of the attack, this version was able to self-replicate within specified networks and transfer via removable stick drives to all kinds of computers. However, like the first version, it would only execute when it detected the specific Siemens PLC configuration it targeted. This version was also loaded with "zero day vulnerabilities" or undiscovered flaws in Microsoft Windows software. These are rare, and can go for hundreds of thousands of dollars each on the open market—indicating either a wealthy attacker, a technically sophisticated attacker, or both. Finally, this stage of the attack was accompanied by stolen digital certificates, which masked the malware as legitimate software and prevented its rejection by updated Windows operating systems.[18]

Once again, the new attack executed once per month, this time speeding up centrifuge rotor speeds, abruptly slowing them to almost a stop, and then speeding them back up again.[19] This occurred over a period of about 50 minutes. Because of the IR-1's supercritical design, the rotor had to pass through certain "critical speeds" before achieving a normal operating pace. Passing through these critical speeds, or "harmonics," could cause rotors to break. While the cascade protection system that Iran had devised could handle one cracked rotor, the problem once again occurred when multiple rotors crashed. This frustrated Iranian engineers immensely; while they had enough centrifuges to keep replacing those that broke, the engineers still had the maddening task of deciphering why the centrifuges were crashing in such volumes.[20]

---

14. "Basic Attack Strategy of Stuxnet 0.5 Rev. 1."

15. Geoff McDonald, Liam O'Murchu, Stephen Doherty, and Eric Chien, "Stuxnet 0.5: The Missing Link," Symantec Security Response, February 2013, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf.

16. Langner, "Stuxnet's Secret Twin."

17. Goodin, "Revealed: Stuxnet 'Beta's' Devious Alternate Attack on Iran Nuke Program."

18. Langner, "Stuxnet's Secret Twin."

19. Ron Rosenbaum, "Richard Clarke on Who Was behind the Stuxnet Attack," *Smithsonian Magazine*, April 2012, http://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/#obL1AHrdHV08K5A0.99.

20. Langner, "Stuxnet's Secret Twin."

Although this attack could only spread between computers attached to the same network or that exchanged files over USB sticks, computers could connect to these networks from hundreds of miles away using remote access or virtual private networks (VPNs). This change to how Stuxnet propagated spelled the beginning of the end as contractors carried Stuxnet-infected laptops to other client sites besides Natanz. Stuxnet would make the jump to that network and lay dormant, not detecting any of the specific technical specifications it was instructed to find.[21] The virus would then be transferred to other computers and USB sticks that would then be carried elsewhere and connected to still other networks. As people remotely accessed infected networks, the virus zoomed to their computer, sometimes actually traveling across continents. Soon, Stuxnet had traveled around the world solely on trusted Internet connections, making its ultimate discovery by a Belarusian security research firm inevitable.

Ultimately, Stuxnet destroyed roughly 1,000 out of a total of 9,000 IR-1 centrifuges at Natanz. This was certainly disruptive to Iranian enrichment efforts, forcing them to spend time and resources investigating the breakages, which in turn delayed nascent plans to expand the plant. Stuxnet also forced Iran to draw on its supply of centrifuges more quickly than it otherwise would have in order to replace those broken by the malware.[22] However, the attack was not an unmitigated success, as Iranian scientists responded to the breakages with actions that reduced further damage, mainly by shutting down centrifuge cascades for months on end. If the cascades were shut down, Stuxnet could not attack; and this decision created enough time and space for public discovery.[23]

BEYOND STUXNET: WHAT COMES NEXT?

The deployment of Stuxnet against the Natanz uranium enrichment facility was unprecedented and gave rise to many important questions about the nature of conflict in cyberspace; after all, never before had a cyber attack caused real, physical consequences at a nuclear facility. However, examining the case of Stuxnet in the nuclear security context demonstrates that Stuxnet was only the beginning. More malicious adversaries attacking less secure targets with less discriminate weapons can achieve far more serious consequences.

Target

A key component of the Stuxnet worm was the target it was intended to impact: a specific device within a well-defended facility that had already been the subject of significant international outcry. The Natanz uranium enrichment facility was part of what many believed to be a clandestine nuclear weapons program and was not supposed to exist. Although initially marketed to the international community as a desert-eradication project, evidence revealed by the National Council of Resistance of Iran (NCRI) in 2002 suggested that the site was actually meant for undeclared uranium

21. Ibid.

22. David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS [Institute for Science and International Security] December 22, 2010 Report," Institute for Science and International Security, February 15, 2011, http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf.

23. Ibid.

enrichment.[24] Satellite imagery and Iranian regime behavior later confirmed this assertion. Because this site was being constructed in secret to conduct illicit activities, security measures surrounding it were intense; in fact, plant employees were not even allowed to discuss their work with local officials. The Atomic Energy Organization of Iran would not even reveal the nature of the site with the local governor's office.[25]

Security was taken so seriously because Iranian authorities knew the site would be a target for foreign governments even before its existence was revealed. Satellite imagery analyzed by the Institute for Science and International Security provided evidence to this point. Photographs showed that the site was constructed entirely underground and that efforts were ongoing to camouflage it from view using earth and cement.[26] Circles visible around the perimeter of Natanz suggested plans to install antiaircraft guns. Underground buildings were built with concrete walls varying between six and eight feet thick—suggesting that they were heavily reinforced. Finally, even the tunnels leading to the underground facilities were constructed in such a way as to protect their contents from missiles fired on top of or directly into the tunnels.[27]

After the existence of Natanz was revealed and confirmed, the IAEA did gain some limited access. However, after Iran purported to suspend uranium enrichment activities in January 2006, the IAEA lost the ability to monitor key items like centrifuge components, assembled centrifuges, and associated equipment. Iran also revoked the IAEA's ability to conduct advanced inspections as permitted in the Additional Protocol. Taken together, this meant that the IAEA's understanding of activities at Natanz deteriorated over time.[28] It also suggested a tightening of security at the Natanz facility itself.

The fact that such a well-defended facility could still be compromised by a cyber weapon should concern the international community. Most nuclear facilities, including nuclear power plants, nuclear materials storage facilities, spent fuel pools, and even some large research reactors are more susceptible to cyber attack than Natanz and would result in more serious consequences should such an attack prove successful. Moreover, these facilities often employ standardized technologies. This means that many different facilities share the same system designs and configurations and rely upon the same technologies from the same small group of vendors. Therefore, if one facility can be hacked, it is likely that others could be too.[29]

---

24. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), 34.

25. Ibid., 36.

26. Paul Brannan and David Albright, "ISIS [Institute for Science and International Security] Imagery Brief: New Activities at the Esfahan and Natanz Nuclear Sites in Iran," Institute of Science and International Security, April 14, 2006, http://isis-online.org/uploads/isis-reports/documents/newactivities.pdf.

27. David Albright and Corey Hinderstein, "The Iranian Gas Uranium Enrichment Plant at Natanz: Drawing from Commercial Satellite Images," Institute for Science and International Security, March 14, 2003, http://isis-online.org/isis-reports/detail/the-iranian-gas-centrifuge-uranium-enrichment-plant-at-natanz-drawing-from-/8#images.

28. Brannan and Albright, "ISIS Imagery Brief."

29. Langner, "Stuxnet's Secret Twin."

Additionally, because the malware was meant to attack only a specific device, the potential for the loss of life or environmental degradation was extremely low. By targeting the operations of the Siemens programmable logic controllers (PLCs), the potential for harm to humans or the environment was significantly lowered. While the Iranian uranium enrichment program certainly experienced a setback, the potential for the theft of nuclear materials or radiological release was extremely limited. This is not necessarily the case at most nuclear facilities.

Intent

Technical analysis of both stages of Stuxnet confirms that the attacker—likely a nation-state—sought to slow or halt Iran's uranium enrichment program and avoid catastrophic damage. For example, the first version of the attack, which attempted to break centrifuges by overpressurizing them, monitored the status of targeted centrifuges very closely. Ralph Langner, an industrial control systems expert who worked to initially decipher Stuxnet, described the code undergirding this stage of the attack as "so engineered that even the slightest oversight or any configuration change" would have rendered the attack useless.[30] This means that the attack would only execute in conditions for which it had been designed to operate.

Looking at the Stuxnet operation in its entirety, Langner also contends that "the attackers were in a position where they could have broken the victim's neck, but they chose continuous periodical choking instead." This suggests that the intent was not to cause massive destruction; rather, it was to reduce the effectiveness of Iranian enrichment, force engineers to spend valuable time and resources on fixing or replacing centrifuges, and perhaps even push Iran to question its ability to develop and field a nuclear program.[31]

Unfortunately, not every deployment of a cyber weapon against a nuclear facility will have as narrow a mission. Terrorist groups have stated their desire to acquire weapons of mass destruction to achieve their aims. For example, Ayman al-Zawahiri, the current leader of al Qaeda, has written forcefully in favor of using nuclear weapons to retaliate against the West and has maintained this position for well over a decade.[32]

Furthermore, fears about the brutal organization Islamic State of Iraq and the Levant (ISIL) obtaining weapons of mass destruction have been growing as the group has ramped up its activities in the past two years. In fact, in March 2016, law enforcement discovered that the same ISIL cell that carried out the horrific Brussels attack that same month were actively surveilling a senior scientist who had access to sensitive areas of a Belgian nuclear research facility.[33] Additionally, ISIL was able to radicalize an employee at the Doel nuclear power plant in Belgium who ultimately left the country to fight for the terrorist organization.[34] Although he was

30. Ibid.

31. Ibid.

32. Mowatt-Larssen, "Al Qaeda's Nuclear Ambitions."

33. Sengupta, "ISIS Nuclear Attack in Europe Is a Real Threat, Say Experts."

34. Karl Vick, "ISIS [Islamic State of Iraq and Syria] Attackers May Have Targeted Nuclear Power Station," *Time*, March 25, 2016, http://time.com/4271854/belgium-isis-nuclear-power-station-brussels/.

killed in Syria, it is clear that this brutal terrorist group has a dangerous foothold in the nuclear space.

Groups like al Qaeda and ISIL would not use cyber weapons as Stuxnet's creators did: as a precise tool to achieve a specific and limited goal in a way that does not threaten human life or the environment. They would leverage the complete destructive power of cyber weapons to achieve their aims. This could include detonating a nuclear device built using materials stolen during a cyber-facilitated theft or achieving serious radiological release by sabotaging a nuclear facility.

Weapon

Stuxnet as a weapon has two important implications for the nexus of cyber and nuclear security. The first is its precision; Stuxnet was engineered to be a precise and discriminate weapon that did not cause physical destruction outside a narrow and specific set of conditions. The second is its availability; when it was first developed, a weapon like Stuxnet could not have been constructed without a nation-state's access to extensive technological, financial, and intelligence resources. As revelations of Stuxnet came to light, so too did its source code, which is now widely available to use in any number of more sinister attacks. When Stuxnet was originally deployed, it required a thorough understanding of nuclear engineering in order to be effective. This may continue to raise the "barrier to entry" for a potential attacker; however, this will depend on the target. Now that almost anyone with sufficient funds can make use of a weapon like Stuxnet, the initial, carefully calibrated deployment of the weapon can no longer be guaranteed—especially where non-state actors are concerned.

Precision

Stuxnet's technological precision was discussed in previous sections, but insight from Richard Clarke, counterterrorism expert and former special advisor to the president of the United States on cyber security, provides evidence that the weapon was also legally precise. He noted in a recent interview, "it very much had the feel to it of having been written by or governed by a team of Washington lawyers."[35] Based upon his knowledge of how government lawyers review proposals for covert action, he pointed to how Stuxnet's design limited its possible physical effects. "The lawyers want to make sure that they very much limit the effects of the action. So that there's no collateral damage," Clarke explained. The fact that Stuxnet may well have been designed with an eye toward laws and norms underlines the extent to which it was designed to have a narrow physical impact and not cause broader destruction.[36]

Ultimately, the weapon behaved as expected and did not cause damage beyond the centrifuges it was built to target. The weapon was painstakingly engineered, exhaustively tested, and only sought one victim: a Siemens PLC. Interrupting the operations of this particular device did not pose a threat to humans or the environment. Even when Stuxnet escaped Natanz, it caused no damage, instead simply shutting itself down in the absence of the specific conditions in which it

35. Rosenbaum, "Richard Clarke."

36. Ibid.

was designed to operate.[37] As a result, there were no serious physical consequences—just a rush in the security community to identify the virus.

Beyond the Nation-State

Cyber weapons are no longer the exclusive purview of nation-states. In the words of the renowned cryptographer Bruce Schneier, "Today's NSA secrets become tomorrow's PhD theses and the next day's hacker tools."[38] Today, determined adversaries can purchase Stuxnet for a fraction of what it cost to develop and use the source code as a template.[39]

Experts agree that this is perhaps the most troubling consequence of Stuxnet—the fact that its code can now be dissected and repurposed into new, possibly more dangerous weapons. Clarke himself has publicly stated that:

> if you're a computer whiz you can take it apart and you can say, "Oh, let's change this over here, let's change that over there." Now I've got a really sophisticated weapon. So thousands of people around the world have it and are playing with it. And if I'm right, the best cyberweapon the United States has ever developed, it then gave the world for free.[40]

Ralph Langner is more doubtful about the level of knowledge an adversary must possess to make use of Stuxnet's code. In an interview with the *Christian Science Monitor*, he stated, "you don't have to be a genius to create a program that works on a control system exactly the way Stuxnet does." Knowing how to copy elements of the code and understanding how to weaponize it for a desired target is now sufficient to make use of one of the most sophisticated cyber weapons ever developed.[41]

Importantly, many of the costs associated with Stuxnet came from the constraints faced by its creators. They hoped Stuxnet would never be discovered, and made every effort to design it appropriately. The largest investments of time and money likely came as a result of efforts to camouflage the attack and make its effects appear to be legitimate mechanical issues.

Furthermore, gathering the requisite intelligence on Natanz was likely not cheap, and required heavy investments from the intelligence community. Attackers seeking to cause destruction and not hide it are unlikely to make similar investments in disguising the effects of their operations, making a copycat attack all the easier.[42]

---

37. Jason Healey, "Stuxnet and the Dawn of Algorithmic Warfare," *Huffington Post*, March 16, 2013, http://www.huffingtonpost.com/jason-healey/stuxnet-cyberwarfare_b_3091274.html.

38. Bruce Schneier, "Cyberweapons Have No Allegiance," *Motherboard*, February 25, 2015, http://motherboard.vice.com/read/cyberweapons-have-no-allegiance.

39. Mark Clayton, "Stuxnet 'Virus' Could Be Altered to Attack U.S. Facilities, Report Warns," *Christian Science Monitor*, December 15, 2010, http://www.csmonitor.com/USA/2010/1215/Stuxnet-virus-could-be-altered-to-attack-US-facilities-report-warns.

40. Rosenbaum, "Richard Clarke."

41. Clayton, "Stuxnet 'Virus.'"

42. Langner, "Stuxnet's Secret Twin."

RECOMMENDATIONS FOR MOVING FORWARD

Armed with Stuxnet's lessons, leaders today can improve global preparedness and construct effective defenses. The following recommendations demand a sustained investment of resources, financial, intellectual, and otherwise; they also constitute much-needed advances toward the comprehensive nuclear security the world needs.

First, and most important, the current approach to cyber security at nuclear facilities must be fundamentally rethought. A new strategy, grounded in technically sound and forward-looking principles, must be developed to meet this dynamic threat. Despite ongoing efforts at the International Atomic Energy Agency, the World Institute for Nuclear Security, the United Nations, Nuclear Security Summits, and various national initiatives, recent years have seen example after example of successful infiltration of nuclear facilities by malware, targeted or otherwise. These cases alone demonstrate the insufficiency of the current approach. In order to defend against the well-resourced, targeted cyber attacks against nuclear facilities that could cause significant damage, a fresh look at what is necessary for defense is required.[43]

In the Stuxnet case, malware was able to infiltrate the facility for two key reasons. First, an organizational overreliance on air gaps to protect networks from infection created a false sense of security, and attackers were able to use this to their advantage. Second, the digital systems employed to keep Iran's IR-1 centrifuges up and running were highly complex and, therefore, highly vulnerable.

A new strategy for cyber security at nuclear facilities must address both of these factors. It could include a reassessment of the effectiveness of commonly relied-upon defense architectures and tools; these findings might lead to the creation of fundamentally new defense techniques and procedures at nuclear facilities. It could also focus on reducing the use of digital technologies at the most critical nodes of the facility, and reducing complexity in the most vital systems. Removing these known vulnerability multipliers from facilities would be an important step toward better security.

Second, nations must invest in response capabilities at home and abroad. Even if perfect policy could be written tomorrow, it would still take several years to implement. During this time, the possibility of a cyber attack with serious physical consequences would still exist. Therefore, every country needs to have a clearly articulated rapid response plan in place, with any provisions necessary to facilitate international cooperation.

Moreover, those countries that benefit from higher numbers of cyber-nuclear experts should work to develop ways to share this expertise with countries that need it in order to prevent or respond to cyber incidents. In terms of prevention, these experts could consult with facility operators on steps that could be taken immediately to improve protections against cyber attacks. If an incident is under way, these same people could make themselves available to help respond or, at the very

43. The Nuclear Threat Initiative has begun this work by developing a set of strategic priorities to guide such a strategy. Please see www.nti.org/about/cyber for more information.

least, to assist with post-incident analysis. The nuclear industry could play an important role in facilitating these connections.

Third, the international community must work to build global human capacity in this area. Achieving a sustainable strategy for mitigating this threat requires sufficient talent to develop and implement it. This aim can be achieved by strengthening the global cyber-nuclear community and facilitating connections across borders, seeking out opportunities to support or incentivize educational programs focusing on the cyber-nuclear nexus, and funding and supporting training programs at home and abroad to improve and build expertise in this area.

CONCLUSION

Although the Stuxnet worm will live in infamy as "the keystroke heard 'round the world," it only represents the beginning in terms of what can be achieved with a cyber attack at a nuclear facility. Stuxnet was an unprecedented weapon into which significant resources were invested. It was crafted to be precise in its destruction and deployed with the specific goal of slowing or halting Iran's nuclear program. It was launched against a highly secure facility and still managed to compromise its defenses.

The more pressing threat today is not that of a targeted action against a country undertaking an illegal nuclear weapons program. It is that determined adversaries with more sinister ambitions will use indiscriminate cyber attacks against less secure, higher-consequence nuclear facilities to facilitate the theft of nuclear materials or a serious act of sabotage. Stuxnet showed the world the art of the possible when it comes to cyber attacks at nuclear facilities; it serves as a valuable reminder that no matter how secure a facility appears, it can still be vulnerable. However, the international community has no shortage of targets and no shortage of potential adversaries seeking to cause destruction.

The international community must heed Stuxnet's wake-up call and start taking steps to better defend itself against this threat.

The South China Sea and Nuclear Deterrence in the Asia Pacific

Brittney Washington[1]

The South China Sea is a point of tension between China and its neighbors due to the sea's natural resources and key maritime shipping routes. Friction continues to grow as China engages in island-building and conducts naval patrols in these contentious waters, while the United States seeks to promote freedom of navigation and support allies by conducting its own patrols and surveillance activity. China's People's Liberation Army (Navy) (PLAN), in an effort to modernize its sea-based deterrent, is investing in its strategic ballistic missile submarine (SSBN) fleet. This paper will consider the role of the South China Sea in China's maritime strategy, specifically whether it will serve as a route for an open-ocean deployment strategy or bastion for PLAN SSBNs. I will draw from the writings of nuclear scholars to discuss how China's investment and deployment of SSBNs might impact nuclear deterrence between China and the United States. This paper will also examine the impact on Sino-Indian nuclear deterrence, considering India's presence as both a maritime and nuclear power in the Pacific region. The paper will conclude by exploring options for confidence-building measures that will minimize the risk of conflict escalation between these three nuclear powers.

INTRODUCTION

President Xi Jinping coined the phrase "the China Dream," an expression that refers to a future in which the People's Republic of China (PRC) has significant regional and global impact vis-à-vis diplomacy, its economy, and military power. The People's Liberation Army (Navy) has a key role in this grand strategy, as Xi calls for China to "do more to take interest in the sea, understand the sea, and strategically manage the sea."[2] Ninety percent of China's foreign trade occurs by sea, and

1. Brittney Washington is a graduate student at the Fletcher School of Law and Diplomacy with a background in Pacific Asia and international security studies.

2. Office of Naval Intelligence, *The PLA Navy: New Capabilities and Missions for the 21st Century* (Washington, DC: Office of Naval Intelligence, 2015), 7.

therefore one of the key maritime priorities for the PRC is protecting sea lines of communications (SLOCS).[3] The South China Sea (SCS), as a vital body of water, is the most contentious.

China, Brunei, the Philippines, Malaysia, Vietnam, and Taiwan all have claims to territory within the SCS. China's claims are the largest; the PRC's nine-dash-line claims encompass the Spratly and Paracel Island chains as well as other land features. Despite growing international opposition and The Hague's recent ruling in favor of the Philippines' rival claims, China continues to increase its naval presence and to build islands in these waters. The United States seeks to uphold freedom of navigation by conducting its own patrols near territory claimed by China, which has resulted in close calls or moments of friction between the PLAN and U.S. Navy that have the potential to result in conflict.[4]

Alarm over the possibility of a conflict between the United States and China due to the current situation surrounding the SCS certainly has implications for strategic stability and nuclear deterrence in the Pacific. As China pursues development of the second leg of its nuclear triad, strategic ballistic missile submarines (SSBNs), to achieve the Chinese leadership's vision of a stronger, modernized PLAN, the SCS may become a bastion or a route for open-ocean deployment. Thus, avoiding miscalculations and misunderstandings between the PLAN and U.S. naval forces will be ever more important. Also, relations between India and China would be impacted; if a nuclear confrontation occurred between India and China, SSBNs would augment China's current deterrent options. The risk of conflict escalation must propel these nuclear powers to establish viable confidence-building measures that will prevent instability in the Pacific.

CHINA'S BALLISTIC MISSILE SUBMARINE FORCE

Chinese strategists identify several factors behind the modernization of China's sea-based deterrent:

- *High Survivability and Stealth:* Investing in SSBNs could give China a more survivable second-strike capability because an adversary cannot easily detect them, unlike land-based missiles.
- *Mobility and Range:* SSBNs are very mobile and have the capacity to reach enemy territory and launch missiles without interference from missile defense systems.
- *International Trends:* Most nuclear weapons states are boosting their sea-based nuclear deterrence capabilities.[5] In fact, of the UN Security Council's permanent five members (P5), the PRC will be the last member to achieve an operational SSBN capability.[6]

3. Ibid.

4. Jim Sciutto, "US Navy to China: We'll Continue Operation in South China Sea," CNN, July 26, 2016, http://www.cnn.com/2016/07/26/politics/china-us-navy-chief-south-china-sea/.

5. Tong Zhao, "China's Sea-Based Nuclear Deterrent," Carnegie Endowment for International Peace, June 30, 2016, http://carnegietsinghua.org/2016/06/30/china-s-sea-based-nuclear-deterrent/j2oc.

6. ChinaPower, "Does China Have an Effective Sea-Based Nuclear Deterrent?," Center for Strategic and International Studies (CSIS), accessed on July 5, 2016, http://chinapower.csis.org/ssbn/. The permanent five members of the UN Security Council are France, the People's Republic of China, Russia, the United Kingdom, and the United States.

According to the U.S. Department of Defense's 2016 annual report to Congress, China has commissioned four second-generation SSBNs, known as the JIN-class SSBNs (Type 094), with an additional submarine under construction.[7] Each JIN-class submarine is equipped with twelve JL-2 submarine-launched ballistic missiles (SLBMs) that can be mated with one to three nuclear warheads.[8] These intercontinental missiles have a range of approximately 7,400 kilometers, which means that, from the South China Sea, they are capable of striking Guam and Hawaii, and (if launched from the mid-Pacific Ocean) the continental United States.[9] The Type 094 submarine shows vast improvements over its predecessor, the *Xia*-class SSBN (Type 092) armed with the JL-1 SLBM, which had a limited range of 1,700 to 2,500 kilometers and never conducted deterrent patrols because the level of noise it emitted could be detected by sonar.[10] The JIN-class submarines are considered China's first credible sea-based nuclear deterrent, and it is possible that the PLAN will build more of these in the future. Admiral Samuel Locklear, former commander of U.S. Pacific Command projected that the PLAN will have eight SSBNs by 2020.[11]

These submarines are currently held at a base on the southern coast of Hainan Island in the South China Sea.[12] Chinese military officials have recently announced that the deployment of its SSBN fleet in the Pacific is inevitable as a result of the United States' deployment of terminal high-altitude area defense (THAAD) antiballistic interceptors in South Korea.[13] As the Chinese government settles on the size of its SSBN fleet and its deployment pattern(s), challenges will arise for maintaining stability in the Pacific.

POSSIBLE DEPLOYMENT PATTERNS AND STRATEGIC STABILITY

China's command over its near seas—specifically whether the PLAN can successfully carry out an anti-access/area denial (A2/AD)[14] strategy that will deny U.S. naval forces entry into these seas

---

7. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, DC: Office of the Secretary of Defense, 2016), 26.

8. Ibid.

9. ChinaPower, "Does China Have an Effective Sea-Based Deterrent?"

10. Lora Saalman, ed., *The China-India Nuclear Crossroads* (Washington, DC: Carnegie Endowment for International Peace, 2012), 3.

11. Senate Committee on Armed Services: Hearings before the committee on U.S Pacific Command Posture, Senate, 114th Cong. 9, 2016.

12. Office of Naval Intelligence, *The PLA Navy: New Capabilities and Missions for the 21st Century,* 14.

13. The U.S. government states that its deployment of THAAD in South Korea is an added defense measure against a potential North Korean missile threat. However the Chinese government believes that THAAD was deployed as a defense measure against China that can track Chinese missile warheads. See Li Bin's "The Security Dilemma and THAAD Deployment in the ROK," Carnegie Endowment for International Peace, August 3, 2016, http://carnegieendowment.org/2016/08/03/security-dilemma-and-thaad-deployment-in-rok/j3j2.

14. Naval experts Toshi Yoshihara and James Holmes define anti-access/area denial (A2/AD) as a tactic that involves using

> military and nonmilitary steps to (1) delay the arrival of U.S. and allied forces in theater; (2) prevent U.S. forces from using bases in the region to sustain military operations (or, failing that, disrupt the use of these bases); and (3) keep U.S. power-projection assets as far away as possible.

and the effectiveness of its command-and-control system—will determine how Chinese SSBNs are deployed.[15] There are two possible strategies: open-ocean patrols versus bastions. Open-ocean patrols would move Chinese SSBNs beyond the first island chain out into the Pacific Ocean. A bastion strategy would deploy SSBNs in near seas; the South China Sea would serve as a sanctuary for these SSBNs, while nuclear attack submarines, surface naval forces, and airpower would prevent adversaries from striking China's SSBN fleet.

Open-ocean patrols align with the PRC's ultimate aim, as expressed in its most recent Defense White Paper, released in 2015, to "shift its focus from 'offshore waters defense' to the combination of 'offshore waters defense' with 'open seas protection.'"[16] Securing offshore waters and protecting the open seas will allow the PRC to fully benefit from the survivability, mobility, and range of its SSBN fleet. As Ambassador Linton Brooks stated in *Strategic Stability and Submarine Operations*, "submarines are survivable and thus stabilizing only when they are at sea."[17] In other words, if the PRC is to have a survivable sea-based deterrent that will provide a credible second-strike capability, these submarines must be able to operate outside of China's near seas.

However, there are several obstacles to pursuing an open-ocean patrol strategy, including reducing noise emission, establishing a well-managed command-and-control system, and, most significantly, overcoming the barrier of U.S. naval antisubmarine warfare (ASW). Although Type 094 submarines are lauded for emitting less noise than its predecessor, the *Xia* class, there are still technological improvements to be made. Chinese and Western analysts concur that the Type 094 is noisier than submarines found in other navies, including those of the United States, Russia, France, and the United Kingdom.[18] This is a major challenge because moving submarines into the Pacific requires stealth in order to reach the designated patrol areas undetected.[19] In addition to the issue of noise, an effective command-and-control system[20] must be put in place that will ensure that the naval officers operating these submarines are able to communicate with civilian leadership and carry out commands. The PLAN has made strides in this area; Chinese nuclear scholar Tong Zhao cites the successful patrols of Chinese nuclear attack submarines through the Indian Ocean to the Gulf of Aden as evidence of improvement. Finally, deploying these submarines into the Pacific would require covert passage through waters that are under the close surveillance of U.S. Navy and allied maritime forces. Professors Toshi Yoshihara and James Holmes reference the U.S. Sound Surveillance System (SOSUS) as an historical example of effective U.S. Navy ASW.

Toshi Yoshihara and James R. Holmes, *Red Star over the Pacific: China's Rise and the Challenge to U.S. Maritime Strategy* (Annapolis, MD: Naval Institute Press, 2010), 6.

15. Ibid.

16. "Full Text: China's Military Strategy," Xinhua Net, May 26, 2015, http://news.xinhuanet.com/english/china/2015-05/26/c_134271001_4.htm.

17. Ambassador Linton Brooks, *Strategic and Submarine Operations: Lessons from the Cold War* (Beijing: Carnegie-Tsingua Center, 2015).

18. Zhao, "China's Sea-Based Nuclear Deterrent."

19. Ibid.

20. The U.S. Department of Defense defines command control as: "The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission." See ChinaPower, "Does China Have an Effective Sea-Based Nuclear Deterrent?"

The United States implemented SOSUS during the Cold War to detect Soviet submarines in the Pacific and successfully tracked these submarines with the help of Japanese naval forces.[21] U.S.-Japan ASW measures have advanced greatly over the years, and Yoshihara and Holmes note the high costs of deploying the Type 094 submarine fleet for open-ocean patrol missions because the PLAN is trying to perfect communication technology to create a sustainable command-and-control system.[22]

The alternative to conducting patrols in the open Pacific is a bastion strategy, which would allow the PLAN to further develop SSBN technology while reducing the threat of detection and/or confrontation with U.S. naval forces. If the PLAN decides to pursue a bastion strategy, then the South China Sea might serve as a sanctuary for Chinese SSBNs in which they could operate under the protection of palace guards, such as nuclear attack submarines, surface forces, and fighter aircrafts.[23]

However, maintaining bastions and palace guards would demand a large amount of resources and would also undermine the critical advantages of the PLAN's SSBNs—survivability, stealth, mobility, and range.[24] Ambassador Brooks notes the vulnerabilities of stationary submarines: "Submarines are survivable and thus stabilizing only when they are at sea . . . submarines in port are easily located and subject to non-nuclear attack."[25] Brooks also draws on the lessons of the Soviet Union and its use of the bastion strategy, pointing out that the strategy was only effective when the USSR had developed the capability to reach enemy territory with its SLBMs from SSBNs positioned in the bastion.[26]

China may choose a bastion strategy over open-ocean patrols until it can further develop SSBN/SLBM technology and its command-and-control system, both of which are necessary for the successful deployment of its SSBN fleet beyond the first island chain. Even as Chinese SSBNs are improved, China may still carry out a bastion strategy because a shift to open-ocean patrols might alarm other naval powers in the Pacific because it would present a "dramatic change in the threat environment."[27]

The South China Sea plays a crucial part in China's strategy; the SCS is deep enough for SSBN operations and, in comparison to the Yellow Sea, has a water temperature and level of salinity that decreases the chances of SSBNs being detected by an adversary's sonar system.[28] Also, in an open-ocean patrol strategy, the SCS would serve as a route that would allow these submarines to enter into the Pacific. The PLAN has already established a submarine base at Hainan Island and will likely continue to use this base going forward.

---

21. Yoshihara and Holmes, *Red Star over the Pacific*, 144.
22. Ibid., 144–145.
23. Ibid.
24. Ibid., 142.
25. Brooks, *Strategic and Submarine Operations.*
26. Ibid.
27. Yoshihara and Holmes, *Red Star over the Pacific*, 142.
28. Zhao, "China's Sea-Based Nuclear Deterrent."

U.S.-CHINA NUCLEAR DETERRENCE AND U.S. STRATEGY

The modernization of China's sea-based deterrent is mostly aimed at deterring U.S. Navy forces and U.S. allies. The 2015 U.S. Office of Naval Intelligence 2015 report "The PLA Navy: New Capabilities and Missions for the 21st Century" states that the PLAN's "JIN/JL-2 weapon system will provide China with the capability to strike targets on the continental United States." If conflict between China and the United States rose to the nuclear level and Chinese land-based missiles were destroyed in a first strike, Chinese SSBNs might be used to carry out a retaliatory strike. Therefore, modernizing Chinese sea-based deterrents is necessary, especially considering China's no-first-use (NFU) policy[29] because the survivability of the SSBN provides China with a second-strike capability that will maintain strategic stability between China and the United States.

However, the South China Sea issue presents obstacles to maintaining peace in the region. As the United States grapples with its rebalance[30] toward the Pacific, China seeks to assert its maritime power to protect the sea territory that it claims. Freedom of navigation patrols conducted by U.S. naval forces in the South China Sea have been called "unprofessional and irresponsible" by the Chinese leadership, who state that the "the U.S. act[s] severely violated Chinese law . . . and undermined the region's peace and stability."[31] Miscalculation or miscommunication might lead to conflict between the two naval powers, especially due to their differences in views on entering a state's exclusive economic zone (EEZ): the United States does not find that United Nations Convention on the Law of the Sea (UNCLOS) or state practice binds nations from conducting military exercises within EEZs, while China believes permission must be given first.[32] Other contingencies involve the United States being drawn into conflict due to a clash between China and the Philippines over resources.[33]

Adding the element of Chinese SSBNs to the South China Sea issues raises the cost of conflict between the United States and China. While the submarines provide China with a second-strike capability, if China in fact creates a bastion in the SCS for these SSBNs, the possibility of a nuclear exchange increases for two reasons. First, a bastion strategy calls for the use of palace guards or

---

29. During the early years of the PRC's nuclear program in 1964, it was determined that China would only use its nuclear weapons in response to a nuclear attack carried out by an adversary, thus no first use (NFU). NFU has been a part of Chinese military doctrine ever since. Chinese nuclear scholar Li Bin explains that China's nuclear weapons are used to counter "nuclear coercion" and that the NFU policy is "based on an understanding that first use of nuclear weapons is not a choice in the real world." See Li Bin's "China's Potential to Contribute to Multilateral Disarmament," *Arms Control Today*, March 3, 2011, https://www.armscontrol.org/act/2011_03/LiBin.

30. After Secretary Hillary Clinton announced the United States' "Pivot to Asia," the Department of Defense stated that 60 percent of U.S. naval forces would be stationed in the Pacific, a change from the 50/50 split of forces between the Pacific and Atlantic. See Ian Rinehart, *The Chinese Military-Overview and Issues for Congress*, U.S. Congressional Research Service Report, RL R44196, March 24, 2016.

31. Sam LaGrone, "China Upset over 'Unprofessional' U.S. South China Sea Freedom of Navigation Operation," *USNI News*, January 31, 2016, https://news.usni.org/2016/01/31/china-upset-over-unprofessional-u-s-south-china-sea-freedom-of-navigation-operation.

32. Bonnie Glaser, "Armed Clash in the South China Sea," Council on Foreign Relations, accessed July 6, 2016, http://www.cfr.org/asia-and-pacific/armed-clash-south-china-sea/p27883.

33. Ibid.

other naval and air forces to defend SSBNs from a conventional attack. Consequently, this would require increased PLAN and People's Liberation Army (Air Force) (PLAAF) forces in the region to protect these assets. An increase in PLAN presence will in turn heighten the possibility for confrontation with U.S. naval forces, which could escalate beyond conventional warfare to nuclear warfare. Second, there is an imminent threat that a Chinese SSBN will be destroyed by a U.S. conventional attack or is actually destroyed in a conventional attack. Zhao lays out the following dilemma:

> If Chinese SSBNs are confronted by rigorous ASW operations, the Chinese leadership may feel that their strategic nuclear deterrent is under direct threat from an enemy's conventional weapons. This would put China in a real dilemma: Should China continue to uphold an unconditional NFU policy? China knows full well that maintaining a policy of unconditional NFU will restrain Chinese response options if an SSBN is sunk by a conventional attack and will very likely encourage the enemy to vigorously track and trail Chinese SSBNs absent the risk of a forceful response.[34]

This second scenario becomes even more severe if China decides to mate nuclear warheads with its SLBMs during peacetime, a practice that most nuclear powers have adopted.[35] If a Chinese SSBN is destroyed by a U.S. conventional attack or if there is the fear that it will be, Chinese leadership may view this as a reason to depart from the NFU policy to protect assets.

If China can successfully conduct open-ocean patrols in the Pacific, then strategic stability might be at stake due to an increase in the number of Chinese nuclear warheads on SSBNs that are capable of striking the continental United States. According to Zhao's research, China's SSBN fleet could include roughly five to eight Type 094 submarines, so that "between 60 and 96 strategic missiles . . . could potentially hit the continental United States," an increase from the 45 intercontinental ballistic missiles (ICBMS) that are currently capable of striking the continental United States.[36] China may be interested in expanding its submarine fleet to a size larger than the anticipated five to eight SSBNs in reaction to expanded U.S. missile defense systems in the Pacific. For example, after Washington announced that it would deploy the terminal high-altitude area defense (THAAD) system in South Korea to intercept North Korean ballistic missiles in the case of a conflict, China responded by stating that the THAAD surveillance system would be able to track Chinese ICBMs, thus creating a strategic imbalance. In order to counteract this imbalance, China announced that it would deploy its SSBNs.[37] Future U.S. missile defense advancement and the growth of Chinese SSBNs in both size and capability have the potential to cause more tension between these two naval powers.

---

34. Zhao, "China's Sea-Based Nuclear Deterrent."

35. Ibid.

36. Ibid.

37. Julian Borger, "China to Send Nuclear-armed Submarines into Pacific amid Tensions with US," *Guardian*, May 26, 2016, https://www.theguardian.com/world/2016/may/26/china-send-nuclear-armed-submarines-into-pacific-us.

INDIA-CHINA NUCLEAR DETERRENCE AND U.S. STRATEGY

Although the advancement of China's nuclear arsenal is primarily focused on ensuring strategic stability with the United States, the modernization of China's sea-based deterrent and the presence of Chinese SSBNs in the South China Sea also has implications for India. China's view of India as a naval power, and India's recognition of China as a land power, play into their perceptions of each other's nuclear arsenals: Saalman identifies Chinese ICBMs, particularly the mobile DF-31, as the largest concern to India because of their range, payload, and "potential to lead to arms racing."[38] Contrarily, China has monitored Indian naval growth and advancement, particularly in "second-strike capabilities, nuclear submarines and aircraft carriers, . . . capabilities that China seeks to either acquire or improve."[39]

However, India's perception of China's naval power may be changing due to the growth of PLAN forces and advancements in China's SSBN/JL-2 missile technology. Chinese nuclear attack submarines have completed a patrol in the Indian Ocean in the past, and the mobility of the Type 094/JIN-class submarine will allow it to do the same. In addition, because these submarines are based on Hainan Island, the PLAN can deploy them quickly into the South China Sea or Indian Ocean, or even launch missiles from the South China Sea that would be capable of striking India. India's strengths include having a favorable position in terms of "geography, maritime capabilities and strategic partnership with the United States."[40] However, China's rapid military growth, including its submarine construction presents a possibility for naval rivalry, especially as both countries have interests in commercial shipping and resources in both the South China Sea and Indian Ocean.

The growth of China's SSBN fleet and other naval forces will heighten India's threat perception of China, but the degree of India's alarm will depend on how China deploys its sea-based deterrent. A bastion strategy in the South China Sea may not heighten India's threat perception as much as an open-ocean strategy that would encompass the Indian Ocean rim (IOR). New Delhi argues that Beijing's actions in the South China Sea are contentious, yet does not agree with the concepts of freedom of navigation and the "right to uninterrupted passage" in coastal waters.[41] Like China, India requires that foreign naval vessels give notice before entering a state's territorial waters or EEZ.[42] These views, as well as perhaps India's desire to maintain its interests in energy resources and trade in the South China Sea by keeping the region stable, may explain why India has decided not to conduct joint patrols in the South China Sea with the U.S. Navy.[43]

---

38. "Introduction," in Saalman, *China-India Nuclear Crossroads*, 3.

39. Lora Saalman, expert on Sino-Indian nuclear relations, unpacks China and India's threat perception. Her findings show that in the past, Chinese strategic analysts were mostly interested in India's naval development, while Indian strategic analysts were mostly concerned by China's land power. Saalman, "Divergence, Similarity and Symmetry in Sino-Indian Threat Perceptions," *Journal of International Affairs* 64.2 (2011): 169–170, 172.

40. Ibid.

41. Abhijit Singh, "India and the South China Sea," *Diplomat*, March 1, 2016, http://thediplomat.com/2016/03/india-and-the-south-china-sea-dispute/.

42. Ibid.

43. Ibid.

If Beijing was to adopt an open-ocean patrol strategy in which Chinese SSBNs were deployed in the IOR, India might perceive this unprecedented action as China's effort to assert itself as the dominant naval power in India's region of influence. In fact, this is a possible red line for India that could lead to an Indian naval buildup in the Indian Ocean and even the South China Sea. Yoshihara and Holmes explain that a presence of SSBNs in the Indian Ocean may prompt New Delhi to undergo a change in naval strategy:

> Several strategic shifts are probable in New Delhi. First, it will pay new attention to the material dimension of naval strategy. Indian governments will orient naval development efforts increasingly toward ASW capabilities, investing in indigenous and foreign-bought diesel and nuclear attack boats, ASW-capable surface vessels, and fixed- and rotary-wing ASW aircraft. . . . Should the PLAN deploy SSBNs in the Indian Ocean . . . the Indian Navy may repay the favor [by] inaugurating SSBN cruises in China's domain.[44]

If there were a situation in which China decided to intensify its A2/AD strategy to a degree that interfered with SLOCS that are of interest to India, this interference could change New Delhi's position on the South China Sea issue and consequently bring about an Indian naval response.

IMPORTANCE OF CONFIDENCE-BUILDING MEASURES

Nuclear scholar and naval experts stress the importance of confidence-building measures, particularly increasing dialogue between the United States, India, and China to avoid a conventional or nuclear crisis. Building multinational maritime partnerships that protect the mutual interests of India, China, and the United States are also emphasized as important confidence-building measures (CBMs).[45]

With regard to U.S.-China maritime relations, Dr. Li Bin, a leading Chinese nuclear scholar, points out the need for military-to-military dialogue. While U.S. and Chinese nuclear scientists and scholars have interacted for decades on strategic nuclear issues, including some military-to-military exchanges in the past, little of this dialogue is now occurring.[46] Bin argues that institutional differences, notably the reluctance of the Chinese military to engage in dialogue, create a barrier between the People's Liberation Army (PLA) and the U.S. Department of Defense. To develop expertise in these areas, Bin suggests that the United States encourage young Chinese military officials to participate in exchange programs at American universities and nongovernmental organizations. This would help them develop expertise in discussing nuclear issues with American counterparts.[47]

---

44. Toshi Yoshihara and James Holmes, "Redlines for Sino-Indian Naval Rivalry," in *Deep Currents and Rising Tides,* ed. John Garofano and Andrea J. Dew (Washington, DC: Georgetown University Press, 2013), 185–209, esp. 195–196.

45. Ibid., 206.

46. Li Bin, "Promoting Effective China-U.S. Strategic Nuclear Dialogue," Carnegie Endowment for International Peace, October 18, 2011, http://carnegieendowment.org/2011/10/18/promoting-effective-china-u.s.-strategic-nuclear-dialogue-pub-45743.

47. Ibid.

Salmaan suggests that India and China engage in Track 1.5 and Track 2 dialogues, which would allow the two countries to set "near term CBMs" to make distinct progress in areas of contention.[48] Track 1.5 dialogues would involve non-governmental organizations and government officials gathering in an informal setting to discuss possible measures for addressing issues. During Track 2 dialogues, non-governmental entities discuss and propose possible recommendations for trust-building between parties involved in a conflict. Salmaan stresses the importance of having these dialogues at the pre-crisis stage rather than trying to address issues post-crisis.[49] In terms of maritime cooperation, India and China can continue to build on their established naval relationship by increasing naval exercises, such as was seen during the November 2003 search-and-rescue operation that the Indian navy participated in that occurred off the coast of Shanghai.[50] She also recommends "expanded cooperation through the Contact Group on Piracy off the Coast of Somalia, the Indian Ocean Naval Symposium," or a newly created maritime organization.[51] Likewise, the United States and China have conducted joint naval exercises in the past, including exercises that center on the Code for Unplanned Encounters at Sea (CUES), which assists both navies in establishing more transparent and fluid communication at sea.[52] Increasing such opportunities for diplomatic exchanges between these three countries will reduce the risks of miscommunication and lower the perception of threats, ultimately diminishing the risk of conflict escalation.

CONCLUSION

The development of China's SSBN force, and the role the South China Sea might have in deployment, add an additional layer to the complex situation arising from China's island building and naval buildup in these contentious waters. If China chooses to use the South China Sea as a bastion or as a route to the Pacific Ocean for the purpose of conducting open-ocean patrols, tensions with the United States and/or India may rise. A bastion strategy would entail a more significant presence of Chinese surface naval forces and aircraft to prevent the U.S. Navy from using ASW capabilities to target China's sea-based deterrent, consequently heightening the possibility of a clash. An open-ocean patrol strategy would allow China's SSBNs to reach the Pacific, providing China with the capability to strike the continental United States and heightening Washington's threat perception of Beijing, which could lead to increased U.S. Navy and its allies ASW capabilities. Open-ocean patrols also have implications for India, a power in the region that has refrained from deploying naval forces in the South China Sea, but may be provoked to do so if China deploys its SSBNs in the Indian Ocean rim as a show of dominance or if China pursues an A2/AD strategy in the South China Sea that would prevent India from taking advantage of SLOCS.

48. Salmaan, "Divergence, Similarity and Symmetry in Sino-Indian Threat Perceptions," 189.

49. Ibid., 189.

50. Ibid.

51. Ibid.

52. Franz-Stefan Gady, "China and US Hold Joint Naval Exercises," November 18, 2015, *Diplomat*, http://thediplomat.com/2015/11/china-and-us-hold-joint-naval-exercise/.

Although there is potential for conflict, confidence-building measures can be critical tools for minimizing distrust and maximizing transparency. The United States, India, and China can benefit from frequent dialogue that occurs pre-crisis rather than post-crisis and focuses on setting manageable, short-term goals. These countries have already begun taking necessary steps in this direction but can enhance current measures by increasing military-to-military exchange between China and the United States and expanding dialogue between India and China to the Track 2 level. Naval cooperation, including conducting joint military exercises that enhance communication between these nuclear powers, is necessary to maintain nuclear stability in the Pacific.

The Impact of the Proliferation Security Initiative on the Interdiction of Weapons of Mass Destruction

Tracey-Ann Wellington[1]

INTRODUCTION

In May 2013, the 10th anniversary high-level political meeting of the Proliferation Security Initiative (PSI) was held in Poland, the site of the launch of the program in 2003. PSI is a "global effort to stop trafficking of weapons of mass destruction (WMD), their delivery systems, and related materials to and from actors of proliferation concern."[2] The initiative was developed as a response to growing proliferation concerns and builds on norms developed within other efforts, such as international treaties and multilateral supplier regimes. PSI does not directly create new international authorities, but does encourage further development of international legal structures that support national interdiction activities, and encourages countries to create national laws that do so as well, with the overall goal of detecting and criminalizing the trafficking of WMD-related materials, equipment, and technology.

In 2003, Australia, France, Germany, Italy, Japan, Netherlands, Poland, Portugal, Spain, and the United Kingdom joined the United States in signing and promoting the PSI. Many other countries, including China, Indonesia and India, have expressed reservations about the initiative, and

1. Tracey-Ann Wellington served as a graduate fellow with the Department of Energy/National Nuclear Security Administration (DOE/NNSA) Office of Nonproliferation and Arms Control. She holds a PhD in Energy Science and Engineering from the University of Tennessee, Knoxville. The views expressed in this chapter are those of the author and do not necessarily reflect the views of the NNSA, the Department of Energy, or the U.S. government.

2. U.S. Department of Defense, "Proliferation Security Initiative," http://www.defense.gov/News/SpecialReports/Proliferation-Security-Initiative.

questioned the international legal justification for the interdiction strategies that it encourages.[3] Currently, 105 countries have committed to the initiative. PSI endorsing states commit to four interdiction principles to create a more efficient and coordinated means of interdicting shipments of WMDs, delivery systems, and related materials transported between states and non-state actors of proliferation concern. These interdiction principles, referred to as Statement of Interdiction Principles (SOIP), state that participating states will:

1. Undertake effective measures, either alone or in concert with other states, for interdicting the transfer or transport of WMDs, their delivery systems, and related materials to and from states and non-state actors of proliferation concern.
2. Adopt streamlined procedures for rapid exchange of relevant information concerning suspected proliferation activity, protecting the confidential character of classified information provided by other states as part of this initiative, dedicate appropriate resources and efforts to interdiction operations and capabilities, and maximize coordination among participants in interdiction efforts.
3. Review and work to strengthen their relevant national legal authorities where necessary to accomplish these objectives, and work to strengthen when necessary relevant international law and frameworks in appropriate ways to support these commitments.
4. Take specific actions in support of interdiction efforts regarding cargoes of WMDs, their delivery systems, or related materials, to the extent their national legal authorities permit and consistent with their obligations under international law and frameworks.[4]

PSI participating governments are responsible for implementing the SOIPs through implementation of domestic laws, including those related to export and transit controls, and regulations governing inspections, seizures, and the disposition of seized goods.[5] International legal frameworks also shape national level behavior, including the antiproliferation provisions present in a wide range of antiproliferation United Nations Security Council resolutions (UNSCRs), such as the Democratic People's Republic of Korea (DPRK) resolutions,[6] the Iran resolutions,[7] and especially

3. Kelsey Davenport, "Proliferation Security Initiative at a Glance," Arms Control Association, June 2013, http://www.armscontrol.org/factsheets/PSI.

4. "Proliferation Security Initiative: Statement of Interdiction Principles," White House, Office of the Press Secretary, last modified September 2003, http://www.state.gov/t/isn/c27726.htm.

5. Kepper Pickard, "The Proliferation Security Initiative," U.S. Department of State briefing, March 2012, https://www.state.gov/strategictrade/documents/organization/190328.pdf.

6. DPRK resolutions include UN Security Council, Resolution 1695 Security Council Condemns Democratic People's Republic of Korea's Missile Launches, Unanimously Adopting Resolution 1695, July 2006, http://www.un.org/press/en/2006/sc8778.doc.htm; UN Security Council, Resolution 1718, Security Council Condemns Nuclear Test By Democratic People's Republic of Korea, Unanimously Adopting Resolution 1718, October 2006, https://www.un.org/press/en/2006/sc8853.doc.htm; and UN Security Council, Resolution 1874, Security Council, Acting Unanimously, Condemns in Strongest Terms Democratic People's Republic of Korea Nuclear Test, Toughens Sanctions, June 2009, https://www.un.org/press/en/2009/sc9679.doc.htm.

7. Iran resolutions include UN Security Council, Resolution 1737, December 2006 http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1737%282006%29; UN Security Council, Resolution 1747 http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1747%282007%29, March 2007; UN Security Council, Resolution 1803, March 2008 http://

Resolution 1540. UNSCR 1540 requires all states to "establish, develop, review and maintain appropriate effective national export and trans-shipment controls."[8] Specifically, under UNSCR 1540, all UN member states are obliged to:

1. Prohibit support to non-state actors seeking WMD and their means of delivery.
2. Adopt and enforce effective laws prohibiting activities involving the proliferation of WMD and their means of delivery to non-state actors.
3. Have and enforce effective measures to reduce the vulnerability of many legitimate activities to misuse in ways that would foster the proliferation of WMD and their means of delivery to non-state actors.[9]

In addition to export controls, the resolution also covers the transfers of WMD-relevant materials, and requires states to adopt and enforce brokering, transit and transshipment controls.[10] UNSCR 1540 encourages "multilateral interdiction cooperation," and provides the legitimacy of global engagements under PSI.[11] To counter the threat of proliferation, operative paragraph 10 of UNSCR 1540 "calls upon all States, in accordance with their national legal authorities and legislation and consistent with international law, to take cooperative action to prevent illicit trafficking in nuclear, chemical or biological weapons, their means of delivery, and related materials."

In addition to the UNSCRs, a range of international legal conventions have emerged or have been strengthened since PSI came into existence that cover the possible modes of conveyance for illicit WMD-related shipments. For example, in the maritime domain, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention) and the 2005 Protocol complement the PSI principles. "The protocol prohibits deliberate maritime shipment of WMD or related materials, equipment, and technology (with the exception of nuclear material and equipment allowed under the Nuclear Nonproliferation Treaty and International Atomic Energy Agency safeguards) . . . the protocol provides for boarding a ship reasonably suspected of proliferation, but only with flag state consent."[12] The flag state consent is only required if the ship is seaward of the territorial sea of an enforcing state (for example, in international waters). Within territorial seas (i.e., 12 nautical miles), the enforcing state can act under its own national authority.

---

www.un.org/ga/search/view_doc.asp?symbol=S/RES/1803%282008%29; and UN Security Council, Resolution 1929, June 2010, https://www.iaea.org/sites/default/files/unsc_res1929-2010.pdf.

8. UN Security Council, Resolution 1540, "Non-Proliferation of Weapons of Mass Destruction," April 2004, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540(2004).

9. Ibid.

10. Catherine B. Dill and Ian J. Stewart, "Defining Effective Strategic Trade Controls at the National Level," *Strategic Trade Review* 1, no. 1 (Autumn 2015).

11. Susan J. Koch, "Proliferation Security Initiative: Origins and Evolution," Occasional Paper No. 9, Center for the Study of Weapons of Mass Destruction, National Defense University, June 2012.

12. "Adoption of the Final Act and any Instruments, Recommendations and Resolutions Resulting from the Work of the Conference: Protocol of 2005 to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation," International Maritime Organization, International Conference on the Revision of the SUA Treaties, November 1, 2005.

In the air domain, the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation of 2010 (Beijing Convention) requires states to "criminalize a number of new and emerging threats to the safety of civil aviation, including using aircraft as a weapon . . . [and] also update provisions to promote cooperation between states in combating terrorism directed against civil aviation."[13] The treaty does not provide actions that states can undertake to prevent the illegal transport of WMD commodities, but, as in the maritime domain, the Beijing Convention affords national actors a range of actions that might be pursued to query suspect shipments or shippers to determine destinations and intent. Because the Beijing Convention needs to be ratified or acceded to by 22 states, it is not yet in force. So far 30 states have signed, but only 14 states have ratified or acceded to the treaty.[14]

One of the key aspects of PSI is that the SOIP, the supplier regimes, related UNSCRs, and certain international conventions all provide the impetus for countries to review and amend, if necessary, their own legislation and related regulations, and to strengthen their capacities to implement antiproliferation measures consistent with multilateral norms.

PSI ACTIVITIES

PSI endorsing states have employed a number of legal, diplomatic, and law enforcement tools to effectively implement the PSI SOIPs. PSI activities can be bilateral, regional, or global, and it facilitates the gathering of a community of experts across the participating states to promote national capacity building. Activities include workshops, political meetings, operational experts group (OEG) meetings, and scenario-based tabletop exercises (TTXs). Over 100 of these activities have been conducted since the inception of the PSI in 2003.[15]

Any PSI endorsing state can host workshops with other PSI endorsing states to assist them in understanding and meeting PSI commitments. These workshops come in a variety of formats, and are used to address critical PSI related topics. In addition to the workshops, on a global basis, PSI high-level political meetings (HLPMs) are held every five years to enable senior officials from all endorsing states to review past activities and related accomplishments, and to discuss future plans. The last HLPM was held in 2013 on the 10th anniversary of the PFI. Mid-level political meetings (MLPMs) also are held periodically to enable experts from endorsing governments to exchange best practices and announce national-level accomplishments. The last MLPM was held in 2016 in Washington, D.C., at which endorsing states reported on interdictions and national-level legal-regulatory reforms designed to enhance their ability to detect and prevent proliferation. The 2016

13. "Beijing Convention and Protocol on Aviation Security Adopted," U.S. Department of State, September 14, 2010, http://www.state.gov/r/pa/prs/ps/2010/09/147110.htm.

14. "Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation Done at Beijing on 10 September 2010," International Civil Aviation Organization, http://www.icao.int/secretariat/legal/List%20of%20Parties/Beijing_Conv_EN.pdf.

15. "Proliferation Security Initiative: Calendar of Events," U.S. Department of State, last modified November 24, 2015, http://www.state.gov/t/isn/c27700.htm.

MLPM also reaffirmed governments' commitment to the initiative, in anticipation of its 15th anniversary. Poland hosted the 2013 HLPM and France will host the 2018 HLPM.

The countries that plan the high- and mid-level meetings are a set of 21 endorsing states that maintain significant interdiction capabilities and expertise, and parallel commitments to deploy them. These countries make up the PSI operational experts group (OEG),[16] and work together to ensure the effectiveness of PSI by:[17]

1. Leveraging related international counter proliferation efforts such as UNSCR 1540.
2. Contributing national customs, law enforcement, military and other security experts and assets to regional interdiction exercises.
3. Hosting PSI meetings, workshops, and exercises with other PSI endorsing states.
4. Working with specific partner states at their request to improve their capacities to combat WMD proliferation.

In addition, several OEG countries came together in 2010 to launch the critical capabilities and practices (CCP) effort. The CCP program is designed to identify and share tools and resources among all PSI endorsing states that would help strengthen their abilities to contribute to interdiction related actions. The CCP addresses four interdiction-related elements: proliferation-related activities that are prohibited, inspection and identification, seizure and disposition, and rapid decisionmaking.

Regional OEG meetings are held for all PSI endorsing states in a given region, and address the challenges and capabilities of the PSI endorsing states in that region. Each meeting allows engagement in a multilateral setting for the OEG and regional PSI endorsers. Regional OEG meetings are held on an ad hoc basis; the last meeting was held in Honolulu, Hawaii, in 2011 for the Asia-Pacific region.

PSI exercises allow relevant communities, such as military, policy, and law enforcement, to practice WMD interdiction decisionmaking strategies in various sea, air, and land scenarios. There is no formal training under PSI; rather, these exercises are held to demonstrate what capabilities currently exist. Designed and scaled to meet the needs of the participating states, the exercises can be bilateral or multilateral. Examples of exercises include military and law enforcement ship boarding and the inspection of suspect cargo in the port (hypothetical case studies), and tabletop exercises (TTXs) that include agency personnel with interdiction responsibilities.

Thirty-eight countries have hosted or cohosted PSI events since 2003. These engagements have made impacts in encouraging other nations to endorse PSI, and adopting the SOIP to improve their interdiction-related activities.

---

16. The OEG members are Argentina, Australia, Canada, Denmark, France, Germany, Greece, Italy, Japan, Republic of Korea, the Netherlands, New Zealand, Norway, Poland, Portugal, Russia, Singapore, Spain, Turkey, United Kingdom, and United States.

17. "Operational Experts Group," Proliferation Security Initiative, accessed May 12, 2016, http://www.psi-online.info/Vertretung/psi/en/04-Operational-Experts-Group/0-operational-experts-group.html.

PSI endorsing countries have utilized TTXs to demonstrate interdiction principles and to provide hands-on learning experiences that mimic real life scenarios and to demonstrate how countries could apply these principles.[18,19] While most often held on a regional basis, TTXs have the added value of attracting participation from multiple regions, thus facilitating the transfer of best practices. They simulate the challenges that could prevent PSI states from effectively accomplishing the PSI SOIP by creating scenarios of where countries of proliferation concern seek to engage in illicit transactions and provide opportunities to explore the legal context of the counter-proliferation regime. Recent TTXs have been held in South Korea, Moldova, and the United Arab Emirates and have simulated air, maritime, and ground interdiction activities. Some achievements that have occurred as a result of the PSI TTXs are:

1. Encouraging countries to endorse the PSI and develop national laws to address the SOIP.
2. Emphasizing the need for bilateral, regional, and international cooperation to interdict WMD-related items across national borders.
3. Highlighting states' progress in the implementation of UNSCR 1540 and the strengthening of strategic trade controls.
4. Stressing that internal and external information sharing of agreements and procedures are key to the success of air interdiction scenarios that require an immediate response and action.

As a result of TTXs, some issues have been brought to light over the years, which enable PSI endorsing states to more effectively prevent and interdict WMD, their means of delivery, and related materials. A few of the issues identified through dozens of TTXs over the past decade show that:[20]

1. The legal justification for interdicting vessels at sea on international and/or territorial waters that are suspected to be carrying WMD-related items fosters substantial debate at the intersection of international maritime law and the various antiproliferation UNSCRs. The TTX process has helped states better understand how to best establish "reasonable grounds" for determining whether or not to engage suspect vessels, and the conditions under which a national government might attempt to do so. TTXs have resulted in countries agreeing in general that the UNSCRs create a mandate to initiate engagement with suspect shippers at sea if, per international maritime law, a ship master's consent is given. This said, legal authorities pertaining to interdictions at sea still vary according to states' interpretation of international laws, and remain the topic of substantial discussion in various PSI forums.
2. There is an identified need for strengthened export control laws as well as uniform port and border security practices across all entry/exit points in order to effectively implement SOIP

18. Proliferation Security Initiative, "Proliferation Security Initiative: Selected Exercises," accessed June 13, 2016, http://www.psi-online.info/Vertretung/psi/en/02-activities/selected-exercises/selected-exercises.html.

19. Proliferation Security Initiative, "Gulf Cooperation Council [GCC] Proliferation Security Initiative Table Top Exercise," March 2012, http://www.state.gov/strategictrade/documents/organization/190375.pdf.

20. Concerns listed are based on reviews of trip reports of past PSI TTXs. http://www.psi-online.info/Vertretung/psi/en/01-about-psi/0-about-us.html.

principals and adhere to proliferation-related UNSCRs. For example, the United States has adopted two catch-alls in its national authorities for conducting WMD interdictions. Limitations on certain activities of U.S. persons (15 C.F.R. § 744.6) "restricts ability for persons to engage in a variety of activities that may support the design, development, production, trade, stockpiling or use of materials that would advance nuclear, missile, chemical, and biological programs."[21] The U.S. Code of Federal Regulations (15 C.F.R. §§ 730—774) adopted the Export Administration Regulations (EAR), which are "broad and intended to reach all parties involved in violations of U.S. export control laws."[22]

3. Almost every PSI endorsing state, including OEG governments, has identified implementation gaps, such as a lack of experience and/or expertise in identifying WMD dual-use items. This has fostered a consensus as to the importance of WMD commodity-focused training.
4. Countries or non-state actors that are party to WMD-related smuggling can intentionally provide misleading or inaccurate information, making it imperative that PSI endorsers collaborate with each other to the maximum degree possible in order to validate and effectively act upon correct information.

LEGAL FRAMEWORKS

PSI emphasizes the importance of developing national legal authorities consistent with international obligations to effectively interdict WMD commodities. PSI has equally brought to the fore the importance of countries adopting new or updating existing legal frameworks that are consistent with one another to the extent possible. This has prompted participating governments to adopt control lists within their regulations that are largely consistent with the multilateral supplier regimes.[23]

Similar to the United States, OEG member states, such as Argentina, Japan and Turkey, have adopted many of these norms. Argentina "regulates weapons of war, and sensitive dual-use materials, used exclusively by the armed forces . . . and the transfer of nuclear, chemical, biological or missile-related material, equipment, technology, technical assistance and services"[24] by Decree

---

21. "Restrictions on Certain Activities of U.S. Persons," 15 C.F.R. 744.6, https://www.gpo.gov/fdsys/granule/CFR-2011-title15-vol2/CFR-2011-title15-vol2-sec744-6/content-detail.html.

22. "Export Administration Regulations," Subchapter C Part 730, 15 C.F.R. 744.6, https://www.gpo.gov/fdsys/pkg/CFR-2012-title15-vol2/pdf/CFR-2012-title15-vol2-subtitleB-chapVII-subchapC.pdf.

23. The four voluntary multilateral supplier regimes are the (1) Nuclear Suppliers Group, formed in 1974, which controls sensitive nuclear-related material equipment and technology; (2) Australia Group, formed in 1985, which controls certain chemicals, biological agents, and dual-use chemical and biological manufacturing facilities and equipment; (3) The Missile Technology Control Regime, formed in 1987, which controls the spread of unmanned delivery systems capable of delivering weapons of mass destruction; and (4) Wassenaar Arrangement, formed in 1995, which controls transfers of conventional arms and related dual-use goods and technologies.

24. "Report of the Argentine Republic on the Implementation of the United Nations Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in all its Aspects," United Nations Programme of

603/92 and its annexes. Japan employs the Foreign Exchange and Foreign Trade Act to control for exports of both arms and dual-use items, and licensing and export regulations to interdict the export of all items applicable to the development of WMD.[25] Turkey has instituted a number of national authorities, including the National Regulations on Permission for the Export of Material and Equipment Used in the Nuclear Field and Related Technology, updated in 2007 (Official Gazette No. 26642); the Export Control of Dual-Use and Sensitive Goods (Wassenaar dual-use goods and Australia Group chemical precursors) (Official Gazette No. 25304); and the Law on Control of the Private Industrial Enterprises Producing War Weapons, Equipment, Vehicles, Ammunition and Explosives (munitions) (Law No. 5201).[26]

Non-OEG member states have also adopted regulations to aid in interdiction efforts. For example, Malaysia passed the Strategic Trade Act in 2010, progressing toward global strategic trade control norms. Armenia has adopted the Criminal Code of the Republic of Armenia, which criminalizes WMD proliferation activities that are prohibited by international treaties to which Armenia is a party. United Arab Emirates adopted the Comprehensive Law on Export Control, which bans the export, reexport, transit, and transshipment of strategic goods, and dual-use items through its territories without a special permit.[27]

INTERDICTION CASE STUDIES

Ship boarding agreements represent one way that the United States has worked with like-minded governments to interdict WMD on the high seas. These agreements provide

> authority on a bilateral basis to board sea vessels suspected of carrying illicit shipments of weapons of mass destruction, their delivery systems, or related materials. These agreements will facilitate bilateral cooperation to prevent such shipments by establishing procedures to board and search such vessels in international waters. . . . [I]f a vessel registered in the United States or the partner country is suspected of carrying proliferation-related cargo, either one of the Parties to this agreement can request of the other to confirm the nationality of the ship in question and, if needed, authorize the boarding, search, and possible detention of the vessel and its cargo.[28]

Action Implementation Support System, May 26, 2006, http://www.poa-iss.org/CASACountryProfile/PoANationalReports/2005@8@argentina-e.pdf.

25. "Security Export Control System in Japan," Ministry of Economy, Trade and Industry, Japan, 2009, http://www.meti.go.jp/policy/anpo/englishpage/overview.pdf.

26. "Turkey's Approach to Arms Control and Disarmament," Republic of Turkey Ministry of Foreign Affairs, accessed May 16, 2016, http://www.mfa.gov.tr/arms-control-and-disarmament.en.mfa.

27. Bryan R. Early, "Export Control Development in the United Arab Emirates; From Commitments to Compliance," Belfer Center, 2009, http://www.belfercenter.org/publication/export-control-development-united-arab-emirates-commitments-compliance.

28. "Ship Boarding Agreements," U.S. Department of State, 2016, accessed June 13, 2016, https://www.state.gov/t/isn/trty/index.htm.

There are currently 11 countries with which the U.S. government has PSI ship boarding agreements: Antigua and Barbuda, Bahamas, Belize, Croatia, Cyprus, Liberia, Malta, Marshall Islands, Mongolia, Panama, and St. Vincent and the Grenadines.

For example, M/V *Light*, a Belizean flagged vessel, suspected of carrying proliferation cargo from North Korea, was bound for Myanmar. It was intercepted in May 2011 by U.S. naval forces, which forced it to return to North Korea.[29] Although the vessel was not inspected, the United States had the legal right to do so due to its ship boarding agreement with Belize.

In another example, in 2013, a consignment was interdicted while en route from China to Egypt; the shipper was listed as a DPRK company. The goods were "labelled as 'machine spare parts,' including relays, 'coils,' connectors and voltage circuit breakers, and were listed as being intended for use in 'freezing carriers,' 'fish factory mother ships,' 'fish-processing machines,' and 'old ships.'"[30] Upon inspection and consultation with several experts, the consignment was found to be spare parts for, or items used in, Scud-B missile systems, which were produced in DPRK.

Most information on actual interdictions is classified, and therefore not published in public sources. Consequently, it is challenging to quantify the number of interdictions that have occurred, even if they cannot be directly attributed to PSI. While there is no single attribution to interdiction activities being PSI dependent, there have been significant advances over the years since PSI was launched.

NEXT STEPS

As states tackle the continually growing issue of the trafficking of WMD-related commodities, new tactics have to be considered. At a recent OEG meeting in April 2016 in London, delegates from all 21 OEG member states came together to discuss new developments in the counterproliferation arena. The OEG provided a number of areas that PSI endorsing states can address as they adopt the PSI principles in their government.

1. Additive manufacturing and intangible technology transfers were identified as two emerging areas that should be addressed. "Countries stressed the need to continue to monitor the advances in materials and processes, and also intangibles such as software and intellectual property, remaining alert to how the different export control regimes look to handle these."[31]
2. The topic of proliferation finance was identified as a key area, and it was stressed that states work with their financial sector in order to improve sanctions enforcement.

---

29. Susan J. Koch, "Proliferation Security Initiative: Origins and Evolution."

30. UN Security Council, "Final Report of the Panel of Experts Submitted Pursuant to Resolution 2207 (2015)," UN Document S/2016/157, http://www.un.org/ga/search/view_doc.asp?symbol=S/2016/157.

31. "Proliferation Security Initiative Operational Experts Group: Chair's Summary," Proliferation Security Initiative, last updated April 14, 2016, http://www.psi-online.info/contentblob/4800426/Daten/6490740/2016_London_PSI_Operational_Experts_Group_Chairs_Summary.pdf.

3. The changing of transportation networks across many jurisdictions and regulatory bodies has also made it more challenging to identify ships of concern and to take the necessary actions in a timely manner.

These areas provide only a snapshot of the current issues facing states as they develop their ability to meet PSI commitments.

CONCLUSION

To determine the success of PSI, it is important to review the SOIP and to evaluate the progress that endorsing states have made in implementing these principles. The number of signers to PSI has increased, and they have changed their legal codes to adhere to SOIP. In addition, PSI promoted a new norm—counterproliferation interdiction, which was a controversial concept before PSI. It, however, has become increasingly accepted as evidenced from details of the interdiction cases mentioned earlier.

The use of TTX to simulate real-world interdictions and other WMD activities allows states to prepare the necessary procedures when actual events arise. TTXs also help states understand the types of laws they need to develop in order to address the legal gaps identified through these exercises. TTXs have shown the need for national agencies to work cooperatively to leverage each other's expertise in order to successfully counter trafficking of WMD-related smuggling. Regional collaboration is also a crucial factor in this global issue, because it helps strengthen supply chains and reduces the ability of proliferators to "port shop," or otherwise find the weakest point in regional supply chains.

Although PSI has had successes, more needs to be done to assist states in adapting to the evolving threat. While it is important that states be party to the international regimes, in order to combat trafficking of WMD commodities, states also need to have robust legal frameworks, and these authorities need to be understood and implemented by the appropriate agencies in a timely manner. The results show that there are ample national authorities being created and amended by the PSI endorsing states, but levels of implementation vary. PSI provides the necessary framework through the SOIP, and a cadre of experts, activities, tools, and 105 endorsing states, that lends confidence to its sustainability in the efforts to combat trafficking of WMD commodities.

The Impact of Hypersonic Glide, Boost-Glide, and Air-Breathing Technologies on Nuclear Deterrence

Rachel Wiener[1]

Russia and China continue to make significant advancements in offensive hypersonic missile technologies and recently announced their intent to insert nuclear weapons payloads on hypersonic glide and/or hypersonic boost-glide delivery vehicles.[2] *Hypersonic glide and boost-glide vehicles are precision-strike weapons designed to penetrate airspace at particular trajectories, speeds, and maneuverability and are capable of being armed with conventional or nuclear explosives.*[3] *At the present time, it is not possible to determine whether the configuration of a hypersonic weapon is conventional or nuclear prior to impact.*[4] *Due to the extremely short time from launch to delivery to target, nuclear-armed hypersonic glide and boost-glide weapons have the*

---

1. Rachel Wiener is a program management and technical analyst for the Department of Energy/National Nuclear Security Administration (DOE/NNSA) Office of Defense Programs supporting advanced research and development for nuclear weapon survivability in hostile environments. The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of any agency of the U.S. government. Examples of analysis performed within this article are only examples. Assumptions made within the analysis are not reflective of the position of any U.S. government entity.

2. Ari Yashar, "Russia, Like China, Tests Nuclear Vehicle to Beat US Defenses," Arutz Sheva, Israel National News, June 25, 2015, http://www.israelnationalnews.com/News/News.aspx/197270.

3. "Hypersonic Missiles: Speed Is the New Stealth," *Economist* (Technology Quarterly: Q2 2013), June 1, 2013, http://www.economist.com/news/technology-quarterly/21578522-hypersonic-weapons-building-vehicles-fly-five-times-speed-sound.

4. Middlebury Institute of International Studies, "Hyper-Glide Delivery Systems and the Implications for Strategic Stability and Arms Reductions," James Martin Center for Nonproliferation Studies, April 2015, http://calhoun.nps.edu/bitstream/handle/10945/45558/Hyperglide%20Final%20Report.pdf?sequence=1.

potential to be used as a strategic first-strike capability.[5] *Compounding the situation, according to publicly available reports, Russian and Chinese hypersonic glide and boost-glide weapons are designed to evade U.S. antiballistic missile defense detection and interdiction.*[6] *According to a congressional commission,*[7] *the United States is currently unable to defend against incoming hypersonic glide and boost-glide vehicles; this poses a problem not only for the United States, but also for its allies that rely on the United States antiballistic missile defense system for protection.*

The United States is also developing hypersonic missile technologies, but, as a matter of current national policy, has limited the arming of these systems to conventional explosives.[8] *Furthermore, U.S. hypersonic development continues to lag behind both Russia and China in various ways, including the overall rate of testing with respect to both Russia and China, and the demonstrated effectiveness of test platforms in the case of China. The totality of Russian and Chinese advancements has a potentially destabilizing effect for U.S. nuclear deterrence posture and presents complex strategic choices for U.S. policymakers. In light of these facts, it is clear that U.S. decision makers must address emerging technology gaps and reexamine policy regarding hypersonic nuclear payloads.*

This paper compares and contrasts the current state of U.S. hypersonic missile technology with Russian and Chinese hypersonic activities and associated nuclear modernization programs. The U.S. hypersonic program, which is disassociated from its own nuclear modernization program, is similarly outlined. This paper also analyzes the dynamics of Russian and Chinese countermoves in response to U.S. antiballistic missile defense deployment. Current U.S. approaches to strategic defense are assessed in light of near-peer activities and several possible courses of action for U.S. policymakers are identified. The overarching conclusions are that the United States should modify its current policy on hypersonic missile armaments, develop countermeasures for hypersonic glide and hypersonic boost-glide vehicles, and work toward the establishment of international norms for the development, deployment, and use of hypersonic weapons; if it does not deploy nuclear armaments on hypersonic delivery vehicles, the United States risks losing the benefits of an effective nuclear deterrent.

---

5. Patrick Tucker, "The Problem with the Pentagon's Hypersonic Missile," Defense One, April 14, 2016, http://www.defenseone.com/technology/2016/04/problem-pentagon-hypersonic-missile/127493/.

6. Jen Judson, "Hypersonic Weapons Threat Looms Large at Missile Defense Symposium," *Defense News*, August 17, 2016, http://www.defensenews.com/articles/hypersonic-weapons-threat-looms-large-at-missile-defense-symposium.

7. According to the congressional Sino-U.S. Economic and Security Review Commission, "The very high speeds of hypersonic weapons, combined with their maneuverability and ability to travel at lower, radar-evading altitudes, make them far less vulnerable than existing missiles to current missile defenses. A capacity to transport nuclear warheads at 10 times the speed of sound exceeds the ability of ballistic missile defenses to prevent them from reaching the U.S." "2016 Annual Report to Congress," U.S.-China Economic and Security Review Commission, https://www.uscc.gov/Annual_Reports/2016-annual-report-congress. Larry Bell has provided commentary on the commission's report in "Russia, China Missiles Overcome all Defenses," NewsMax, May 16, 2016, http://www.newsmax.com/LarryBell/cold-war-dod-putin-missiles/2016/05/16/id/728965/.

8. Amy Woolf, "Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues," Congressional Research Service, February 24, 2016, https://fas.org/sgp/crs/nuke/R41464.pdf.

INTRODUCTION: OVERVIEW OF HYPERSONIC TECHNOLOGY

A hypersonic[9] vehicle flies through the atmosphere below 90 kilometers at speeds above Mach 5. While many types of hypersonic vehicles slated for civilian use continue to be developed, this paper focuses exclusively on the examination of hypersonic delivery platforms for nuclear and conventional missiles. There are three known types of hypersonic delivery platforms intended for weaponized uses under current development: glide, boost-glide, and air-breathing vehicles.

A hypersonic glide vehicle takes flight attached to a single-stage rocket that eventually separates from the booster and allows the weapon to fly unpowered to the target.[10] The concept for hypersonic glide was first studied as a way to extend the range of ballistic missiles, but has yet to be used operationally in this form. Instead, the underlying aerodynamic principles are being applied to maneuverable reentry vehicles, or MARVs, to increase precision-strike accuracy.[11] The initial goal of hypersonic glide technology sought to create a weapon so fast and precise that it relied on the raw force of impact to destroy a fixed target, such as a missile silo.[12] Advancements in aerodynamic lift now allow hypersonic glide vehicles to be highly maneuverable and carry explosive payloads to their targets in a nonballistic trajectory that is unpredictable.[13]

Hypersonic boost-glide vehicles take flight attached to a multistage rocket that separates from the vehicle in two or three stages. Each stage of separation utilizes a new set of engines that further boosts the vehicle into the upper atmosphere at an accelerated rate, before the rocket separates completely and the vehicle flies unpowered to the target. Conceptually, boost-glide allows the vehicle to skim the surface of the upper atmosphere and glide toward a target at a flat angle that is undetectable by antiballistic missile defense systems. Hypersonic boost-glide technology produces a weapon that is incredibly fast and precise, and that flies on a trajectory believed to be outside the range of radar coverage necessary for tracking and interdiction.[14]

---

9. In aerodynamics, a hypersonic speed is one that is highly supersonic reaching speeds of Mach 5 and above. Mach 5 is equivalent to 6,200 kilometers per hour (km/h), which is 3,853 miles per hour (mph) at sea level and 5,300 km/h (3,293 mph) at high altitudes (where the colder, thinner air means the speed of sound is lower). The study of hypersonic speed is not a new phenomenon. In fact, the physics has been applied in a variety of flight dynamics applications for decades. For example, the average velocity of a Minuteman III multistage intercontinental ballistic missile (ICBM) built in 1970 is about 7 kilometers per second (25,200 km/h; 15,659 mph) or Mach 20.

10. Debalina Ghoshal, "The Hypersonic Glide Vehicle Arms Race: Analysis," *Eurasia Review*, May 10, 2016, http://www.eurasiareview.com/10052016-the-hypersonic-glide-vehicle-arms-race-analysis/.

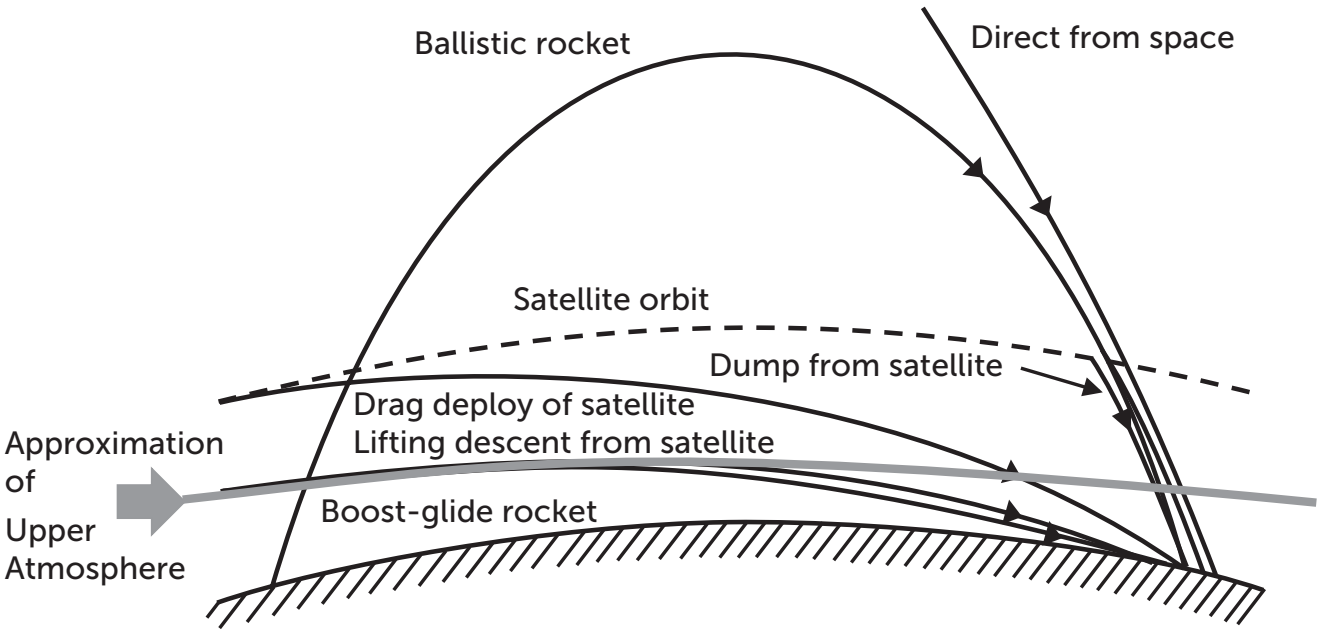
11. Lauren Caston, Robert Leonard, et al., "The Future of the U.S. Intercontinental Ballistic Missile Force," Rand Corporation, 2014, http://www.rand.org/content/dam/rand/pubs/monographs/MG1200/MG1210/RAND_MG1210.pdf.

12. William Broad and David Sanger, "Race for Latest Class of Nuclear Arms Threatens to Revive Cold War," *New York Times*, April 16, 2016, http://www.nytimes.com/2016/04/17/science/atom-bomb-nuclear-weapons-hgv-arms-race-russia-china.html?_r=0.

13. Zachary Putnam, *Improved Analytical Methods for Assessment of Hypersonic Drag-Modulation Trajectory Control*, Georgia Institute of Technology, March 2015, http://www.ssdl.gatech.edu/papers/phdTheses/PutnamZ-Thesis.pdf.

14. Bruce Dorminey, "Russian Hypersonic Glider Weapon Would Easily Penetrate U.S. Defenses, Says Expert," *Forbes*, June 14, 2016, http://www.forbes.com/sites/brucedorminey/2016/06/14/russian-hypersonic-glider-weapons-would-easily-penetrate-u-s-defenses-says-expert/#5804880b1add.

Figure 1. Comparative Trajectories of Atmospheric Reentry Vehicles



Note: Traditional ballistic missiles radar detection methods are aimed at altitudes above the upper atmosphere. The trajectories of hypersonic glide, boost-glide, and air-breathing vehicles (denoted as "Boost-glide rocket" in the graphic) increase the difficulty of tracking and interdiction.

Source: *Space Handbook: Astronautics and Its Applications—Staff Report of the Select Committee on Astronautics and Space Exploration* (Washington, DC: Government Printing Office, 1959), chap. 13 ("Atmospheric Flight"), accessed September 15, 2016, at the National Aeronautics and Space Administration Historical Archives, http://history.nasa.gov/conghand/atmosphe.htm.

Hypersonic air-breathing vehicles take flight attached to a rocket dropped from an aircraft that is accelerated to high speeds and use a unique type of jet engine called a scramjet to sustain flight.[15] Scramjet technology offers a considerable increase in speed and range of motion, and a sizeable decrease in altitude,[16] which reduces flight times to long distance locations to less than one hour.[17] While comparable to the known flight times of deployed ballistic missiles, hypersonic air-breathing vehicles have the advantage of depressed trajectories, flexible recall, and en route redirection ideal for stealth delivery of a nuclear or conventional missile.[18]

---

15. The term scramjet is shorthand for a supersonic combusting ramjet engine, a variant of a ramjet jet engine. In a ramjet engine, external combustion takes place within air that is flowing at subsonic speeds. Ramjet provides a simple, light propulsion system for high-speed flight, while a scramjet provides high thrust and low weight for hypersonic flight speeds. National Aeronautics and Space Administration, "Ramjet/Scramjet Thrust," NASA Glenn Research Center, last updated May 5, 2015, https://www.grc.nasa.gov/www/k-12/airplane/ramth.html.

16. Committee on Hypersonic Technology for Military Applications, "Hypersonic Technology for Military Applications (U)," Air Force Studies Board National Research Council, April 14, 1989, http://www.dtic.mil/dtic/tr/fulltext/u2/a208696.pdf.

17. Theoretical projections place the top speed of a scramjet between Mach 12 (8,400 mph; 14,000 km/h) and Mach 24 (16,000 mph; 25,000 km/h). For comparison, the orbital speed at 200 kilometers (120 miles) low-earth orbit is 7.79 kilometers per second (17,400 mph; 28,000 km/h).

18. Committee on Hypersonic Technology for Military Applications," Hypersonic Technology for Military Applications (U)," Air Force Studies Board National Research Council, April 14, 1989, http://www.dtic.mil/dtic/tr/fulltext/u2/a208696.pdf.

OVERVIEW OF CURRENT RUSSIAN, CHINESE, AND U.S. HYPERSONIC DEVELOPMENTS

It is probable that the rate of Russian and Chinese technological advancements, coupled with their publically acknowledged directives to arm hypersonic glide and hypersonic boost-glide vehicles with nuclear weapons, may lead to a technological imbalance capable of upending the nuclear deterrent that has been maintained for more than half a century.

Russia, China, and the United States are engaged in hypersonic arms development, each with different systematic approaches for success seemingly dependent on a variety of country-specific factors, including: technological capability, the role of the technology in broader military modernization efforts, and perceived or derived policy implications for the deployment and use of the technology.[19] According to publicly available reports, Russia has developed one or more hypersonic glide vehicles, China has developed one or more hypersonic boost-glide vehicles, and the United States has experimented with hypersonic glide, boost-glide, and air-breathing vehicles.[20] For decades, the development of hypersonic technology for military purposes remained stagnant, due to the considerable aerodynamics challenge of achieving and sustaining flight at a low trajectory and fast speeds, as well as the lack of a geopolitical strategic driver—that is, until recently. The perception of U.S. and Western interventionism in Eastern Europe and the Asia Pacific appear to have radically accelerated Russia and China's timeline for initial operational capability to the mid-2020s.[21] Frequent flight tests featuring steady technological improvements continue to demonstrate Russia and China's ability to meet their stated timelines for initial operational capability. At the time of this writing, the most recent flight tests for both nations occurred the week of April 17, 2016. On April 19, Russia launched its first successful flight of the Yu-71 hypersonic glide vehicle; three days later, on April 22, China launched its seventh successful flight of the DF-ZF hypersonic boost-glide vehicle.[22] To put this into perspective, the last successful U.S. hypersonic test flight was in 2011 and its last known flight test was in 2014.[23] Two additional

19. Rudy Panko, "The Hypersonic Arms Race: US, Russia and China Compete to Revolutionize Warfare," *Russia Insider*, March 5, 2016, http://russia-insider.com/en/military/hypersonic-arms-race-us-russia-compete-revolutionize-warfare/ri13191.

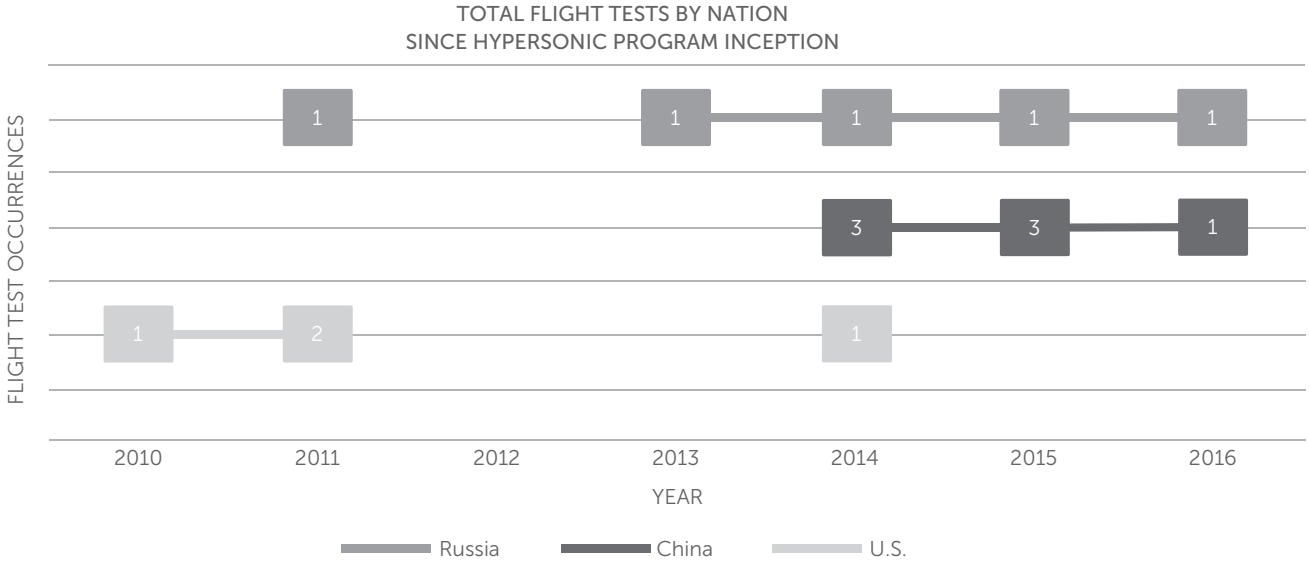
20. Erika Solem and Karen Montague, "Updated: Chinese Hypersonic Weapons Development," Jamestown Foundation, April 21, 2016, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=45313&#.V9B9jKpTGUk.

21. Pavel Podvig, "Blurring the Line between Nuclear and Nonnuclear Weapons: Increasing the Risk of Accidental Nuclear War?," *Bulletin of the Atomic Scientists* 72, no. 3 (2016): 145–149, http://www.tandfonline.com/doi/full/10.1080/00963402.2016.1170363; Timothy Heath and Andrew S. Erickson, "Is China Pursuing Counter-Interventionism?," *Washington Quarterly* (George Washington University Elliott School of International Affairs) 38, no. 3 (2015): 143–156.

22. Bill Gertz, "Russia Tests Hypersonic Glide Vehicle on Missile," *Washington Free Beacon*, April 22, 2016, http://freebeacon.com/national-security/russia-tests-hypersonic-glide-vehicle/; Bill Gertz, "China Successfully Tests Hypersonic Missile," *Washington Free Beacon*, April 27, 2016, http://freebeacon.com/national-security/china-successfully-tests-hypersonic-missile/.

23. Tariq Malik, "US Military Blows Up Hypersonic Weapon after Failed Test Launch," *Space*, August 26, 2014, http://www.space.com/26944-us-military-hypersonic-weapon-test-explodes.html.

Figure 2. Comparative Rate of Frequency for Known Flight Tests of Russian, Chinese, and U.S. Hypersonic Glide and Hypersonic Boost-Glide Vehicles, by Year



flight tests are planned for 2017 and 2019; however, the size and scope of the U.S. hypersonic program indicates that these tests are focused on technological feasibility, not operational deployment.

RUSSIA

Russia has developed at least one hypersonic glide vehicle[24] intended for operational deployment in the mid-2020s[25] and appears to be considering the option of deploying its hypersonic glide vehicle with nuclear missiles, as well as conventional explosive missiles.[26] At the time of this

24. The Russian hypersonic glide case study presented in this paper focuses exclusively on the Yu-71 hypersonic glide vehicle due to an abundance of information provided by credible sources in publicly available literature; however, scholars should not dismiss emerging reports regarding the existence of the Yu-74 hypersonic glide vehicle. Also see Tom Batchelor, "Russia Testing Hypersonic Nuclear Glide That Holds 24 Warheads and Travels 7,000 mph," *Express*, June 15, 2016, http://www.express.co.uk/news/world/680167/Russia-tests-Yu74-hypersonic-nuclear-glider-capable-carrying-24-atomic-warheads.

25. Borris Obnosov, general director of the Tactical Missile Systems Corporation, reportedly announced Russia would build its first air-launched hypersonic missiles before 2020. The Sputnik News Agency, RIA Novosti's International Brand, detailed the announcement in a news broadcast. Zachary Keck of *The Diplomat* has carried the story to the United States. Zachary Keck, "Russia Will Build First Hypersonic Missile Before 2020," *Diplomat*, November 14, 2014, http://thediplomat.com/2014/11/russia-will-build-first-hypersonic-missile-before-2020/.

26. James Acton, subject matter expert on hypersonic technology, assesses that Russia and China are evaluating options of deploying their respective hypersonic technologies in nuclear, as well as conventional, configurations. James Acton, "Silver Bullet," Carnegie Endowment for International Peace, 2013, http://carnegieendowment.org/files/cpgs.pdf. For more information see Bruce Dorminey, "Russian Hypersonic Glider Weapons Would Easily Penetrate

writing, it is unknown whether Russia is also undertaking parallel development for hypersonic boost-glide and air-breathing vehicles, or what its intentions for conventional or nuclear armaments on these types of platforms might be. In 2011, Russia conducted a flight test of its first hypersonic glide prototype, the Yu-71 (referenced in select documents as the 3M22 Zircon). Five flight tests for the Yu-71 have reportedly occurred over Russian territory.[27] During each test, the Yu-71 was attached to a two-stage SS-19 intercontinental ballistic missile (ICBM) capable of delivering multiple nuclear warheads weighing upwards of 9,260 pounds.[28] *Jane's Intelligence Review* indicated that complications in the boost-separation stage caused the first four flight tests to fail.[29] The most recent test on April 19, 2016, was successful, indicating that the problems with the critical boost-separation stage have been corrected.[30] Precision-guidance systems repositioned the rocket upon reaching the edge of the upper atmosphere and successfully glided the vehicle to its designated impact area.[31] The April 19 test also demonstrated evasive maneuverability at speeds of Mach 6 or greater.[32]

Hypersonic glide vehicles play a specific role in Russia's nuclear modernization efforts.[33] The Yu-71 is one part of an ongoing, escalated effort by the Kremlin to overcome U.S. antiballistic missile defenses, known as Project 4202.[34,35] Project 4202 has committed to developing a limited supply of nuclear-armed hypersonic glide vehicles by 2020 and deploying 24 or more hypersonic

---

U.S. Defenses, Says Expert," *Forbes*, June 14, 2016, http://www.forbes.com/sites/brucedorminey/2016/06/14/russian-hypersonic-glider-weapons-would-easily-penetrate-u-s-defenses-says-expert/#33f099c71add.

27. Pavel Podvig and Alexander Stukalin trace the flight tests of the Yu-71 to December 2011, September 2013, September 2014, and February 2015 at the Dombarovsky missile base located in Orenburg, a transcontinental city straddling Russia's border with Kazakhstan. Pavel Podvig and Alexander Stukalin, "Russia Tests Hypersonic Glide Vehicle," *Jane's Intelligence Review*, June 2015. For a table of the tests, see Pavel Podvig, "Summary of the Project 4202 Developments," *Russian Forces* (blog), June 16, 2015, http://russianforces.org/blog/2015/06/summary_of_the_project_4202_de.shtml. The most recent flight test occurred after Podvig's publications. For information on the April 2016 test, see Bill Gertz, "Russia Tests Hypersonic Glide Vehicle on Missile," *Washington Free Beacon*, April 22, 2016, http://freebeacon.com/national-security/russia-tests-hypersonic-glide-vehicle/.

28. "Yu-71 and Checkmating the Prompt Global Strike," Southfront, July 7, 2015, https://southfront.org/yu-71-and-checkmating-the-prompt-global-strike/. For SS-19 ICBM specifications, see Martin Seiff, "Russia Test-Fires RS-18 Stiletto," *Space War*, October 25, 2005, http://www.spacewar.com/news/icbm-05f.html.

29. Kazakhstan. Pavel Podvig and Alexander Stukalin, "Russia Tests Hypersonic Glide Vehicle."

30. "Test Successful: Russian Yu-71 Hypersonic Manoeuvring Warhead for the New SARMAT ICBM," Katehon, April 21, 2016, http://katehon.com/news/test-successfull-russian-yu-71-hypersonic-manoeuvring-warhead-new-sarmat-icbm.

31. Reuben Johnson, "China and Russia Take Aim at THAAD with Hypersonic Programmes," *Jane's Intelligence Report*, May 10, 2016, http://www.janes.com/article/60156/china-and-russia-take-aim-at-thaad-with-hypersonic-programmes.

32. Ibid.

33. Ghoshal, "The Hypersonic Glide Vehicle Arms Race: Analysis."

34. Jeffrey Shapiro, "Russia Launching New Hypersonic Missile to Carry Nuclear Warheads," *Washington Times*, June 26, 2015, http://www.washingtontimes.com/news/2015/jun/26/russia-launching-new-hypersonic-missile-carry-nucl/.

35. Elbridge Colby, *Nuclear Weapons in the Third Offset Strategy: Avoiding a Nuclear Blind Spot in the Pentagon's New Initiative* (Washington, D.C.: Center for a New American Security, 2015), https://s3.amazonaws.com/files.cnas.org/documents/Nuclear-Weapons-in-the-3rd-Offset-Strategy.pdf.

glide vehicles by 2025. Reports indicate that Russia could potentially use the RS-28 ICBM, currently in production, to carry the Yu-71 and successive hypersonic glide vehicles.[36] Russia views Project 4202 and its hypersonic glide subprogram as an essential means for gaining and retaining credibility as a major military power,[37] while counteracting the conventional superiority of the United States and the North Atlantic Treaty Organization (NATO).[38]

The development of hypersonic glide technology is one aspect of Russia's much larger nuclear modernization effort.[39] Russia is modernizing and recapitalizing its entire arsenal of strategic nuclear weapons and delivery systems for land, sea, and air operations.[40] Hans Kristensen and Robert Norris of the Federation of American Scientists suggest that Moscow intends to phase out and replace all Soviet-era nuclear systems in the next decade, although perhaps at a less than one-for-one basis.[41] They note Russia is producing three new land-based missiles, including an SS-27 ICBM modified to carry multiple warheads aimed at different targets.[42] Eight Borei-class ballistic submarines are also reportedly under development, each able to launch 16 missiles and carry up to six independently targetable warheads.[43] A short-range nuclear-capable cruise missile, the Iskander-M SS-26, appears to be nearing operational status.[44,45] Additionally, a Yasen-class nuclear-powered guided-missile attack submarine is reportedly about to enter service, along with a long-range cruise missile potentially equipped for nuclear weapons.[46,47]

---

36. The Sarmat, a liquid-fueled ICBM able to carry multiple warheads, is expected to come into service in 2018. For more information see the Pravada Report entitled "Russia to launch Sarmat monster ICBM towards Hawaii," published January 7, 2016, http://www.pravdareport.com/russia/kremlin/01-07-2016/134903-sarmat_missile-0/.

37. "Russia Overview," Nuclear Threat Initiative, accessed August 15, 2016, http://www.nti.org/learn/countries/russia/.

38. Project 4202 is a demonstrated military reprioritization to field nuclear hypersonic glide vehicles, as well as a substantial inventory of tactical nuclear weapons, nuclear weapons–carrying platforms, and an increasing inventory of theater-range tactical nuclear technologies. Shapiro, "Russia Launching New Hypersonic Missile to Carry Nuclear Warhead." Also see Ghoshal, "The Hypersonic Glide Vehicle Arms Race: Analysis."

39. In addition to the information contained in this paragraph, the Russian bomber force is being upgraded. The Su-34 Fullback fighter-bomber is replacing 1970s-era planes as a platform for tactical nuclear strikes. Plans for a relatively slow but super-stealthy flying wing known as the PAK-DA are also under way. John Mecklin, "Disarm and Modernize," Foreign Policy, March 24, 2015, http://foreignpolicy.com/2015/03/24/disarm-and-modernize-nuclear-weapons-warheads/.

40. "Russia Overview," Nuclear Threat Initiative.

41. Hans Kristensen and Robert Norris, "Russian Nuclear Forces, 2016," *Bulletin of the Atomic Scientists* 72, no. 3 (2016): 125–134, http://www.tandfonline.com/doi/pdf/10.1080/00963402.2016.1170359.

42. Ibid.

43. Ibid.

44. "Weapons of Mass Destruction (WMD): 9K720 Iskander-M (SS-26 Stone)," Global Security, accessed September 1, 2016, http://www.globalsecurity.org/wmd/world/russia/ss-26.htm.

45. Dmitry Litovkin, "Top 3 New Acquisitions of the Russian Armed Forces in 2013," Russia Beyond the Headlines, February 24, 2014, http://rbth.com/defence/2014/02/24/top_3_new_acquisitions_of_the_russian_armed_forces_in_2013_34505.html.

46. Dave Majumdar, "Russia's Next Super Submarine Is Almost Ready for War," *National Interest*, March 27, 2016, http://nationalinterest.org/blog/the-buzz/russias-next-super-submarine-almost-ready-war-15610; "Weapons of Mass Destruction (WMD): Kh-101/ Kh-102," Global Security, accessed September 1, 2016, http://www.globalsecurity.org/wmd/world/russia/kh-101.htm.

47. Kristensen and Norris, "Russian Nuclear Forces, 2016."

CHINA

China has developed at least one hypersonic boost-glide vehicle intended for operational deployment in the mid-2020s and appears to be considering the option of deploying the system with nuclear warheads, as well as conventional explosives.[48] At the time of this writing, it is unknown whether China is also undertaking a parallel development for hypersonic glide and air-breathing vehicles. In 2014, China conducted a flight test of its first hypersonic boost-glide prototype, designated the DF-ZF.[49] Seven flight tests of the DF-ZF[50] have since occurred over China territory.[51] Furthermore, it is unknown which multistage rocket(s) have been used to propel the DF-ZF into the upper atmosphere.[52] However, China has affirmed that the hypersonic boost-glide vehicle can be lifted by a variety of strategic ballistic missiles including the DF-11, -15, -16, -21, and -26 variants.[53] Erika Solem and Karen Montague of the Jamestown Foundation reported that six of the seven flight tests glided to the designated impact area successfully.[54] The April 22, 2016, test of the DF-ZF demonstrated a hypersonic boost-glide vehicle capable of extremely evasive maneuvers at speeds of Mach 10 or greater.[55]

Hypersonic boost-glide vehicles play a specific role in China's nuclear modernization efforts. The DF-ZF is part of an ongoing, escalated effort to overcome U.S. antiballistic missile defenses. China has repeatedly expressed substantial concerns about the U.S. antiballistic missile defense system and is also troubled by U.S. support to its regional allies in the placement of additional antiballistic missile safeguards. The planned operational deployment of the DF-ZF in the mid-2020s represents a noteworthy development for the People's Liberation Army Rocket Force's ability to penetrate the layered antimissile defense system of the United States and its allies.[56] According to Bill Gertz, U.S.

---

48. Bill Gertz, "China Successfully Tests Hypersonic Missile," *Washington Free Beacon*, April 27, 2016, http://freebeacon.com/national-security/china-successfully-tests-hypersonic-missile/.

49. This vehicle is also sometimes referenced as the Wu-14. See Erika Solem and Karen Montague, "The Ultimate Guide to China's Hypersonic Weapons Program," *National Interest*, May 3, 2016, http://nationalinterest.org/blog/the-buzz/the-ultimate-guide-chinas-hypersonic-weapons-program-16029.

50. Consolidation of the hypersonic boost-glide program into the 10th Research Institute likely facilitated the remarkably quick development of the DF-ZF. China's 10th Research Institute, also known as the Near Space Flight Vehicle Research Institute, is the sole entity responsible for the development of boost-glide technology. The Near Space Flight Vehicle Research Institute is housed under the China Aerospace Science Industry Corporation (CASIC). For more information see Mark Stokes and Dean Cheng, "China's Evolving Space Capabilities: Implications for U.S. Interests," Project 2049, April 26, 2012, https://project2049.net/documents/uscc_china-space-program-report_april-2012.pdf.

51. Public reports indicate that the DF-ZF prototypes were launched at the Wuzhai Space and Missile Test Center, also known as Base 25, located in Shanxi Province in central China.

52. Reuben Johnson, "China and Russia Take Aim at THAAD with Hypersonic Programmes."

53. Solem and Montague, "The Ultimate Guide to China's Hypersonic Weapons Program."

54. Ibid.

55. Franz-Stephan Gady, "Should the Pentagon Fear China's Newest Weapon?," *Diplomat*, August 25, 2015, http://thediplomat.com/2015/08/should-the-pentagon-fear-chinas-newest-weapon/.

56. Ibid. See also Shannon Tiezzi, "The New Military Force in Charge of China's Nuclear Weapons," *Diplomat*, January 5, 2016, http://thediplomat.com/2016/01/the-new-military-force-in-charge-of-chinas-nuclear-weapons/.

intelligence officials have assessed China's plans to use the DF-ZF as a nuclear delivery platform,[57] and may be considering the option to use the hypersonic boost-glide vehicle as a conventional strategic strike weapon.[58]

Similar to Russia, the development of hypersonic boost-glide technology is one aspect of China's larger nuclear modernization efforts. China is recapitalizing its arsenal of modern strategic nuclear weapons and delivery platforms for land, sea, and air operations. Kristensen suggests that China is the only member of the Nuclear Nonproliferation Treaty (NPT)–declared nuclear weapons states that is increasing the overall size of its nuclear weapons arsenal.[59] The U.S. Department of Defense (DoD) notes that the People's Liberation Army is replacing its older liquid-fueled missiles with longer-range, road-mobile solid-fuel missiles based at new or upgraded garrisons,[60] considerably increasing the survivability of China's land-based arsenal.[61] Forty-eight JL-2 ballistic submarines are currently undergoing deployment, each able to launch 12 missiles,[62] tripling China's nuclear launch capacity at sea.[63] A long-range tactical nuclear-capable cruise missile, the DH-20, appears to be nearing operational status. China has not confirmed the number of DH-20 cruise missiles under development; however, any production of nuclear-armed air-launched cruise missiles would mark a significant change in China's deterrence posture.[64]

UNITED STATES

The United States has experimented with hypersonic glide, boost-glide, and air-breathing vehicles since the inception of its conventional prompt global strike (CPGS) program in 2003. According to the DoD, the CPGS program funds the design, development, and acquisition of guidance systems, boosters, mission planning capabilities, mission enabling capabilities, reentry systems, and payload

57. Gertz, "China Successfully Tests Hypersonic Missile."

58. Bill Gertz, "Stratcom: China Moving Rapidly to Deploy New Hypersonic Glider," *Washington Free Beacon*, January 22, 2016, http://freebeacon.com/national-security/stratcom-china-moving-rapidly-to-deploy-new-hypersonic-glider/.

59. Hans Kristensen, "Nuclear Weapons Modernization: A Threat to the NPT?," Arms Control Association, accessed September 7, 2016, https://www.armscontrol.org/act/2014_05/Nuclear-Weapons-Modernization-A-Threat-to-the-NPT.

60. U.S. Department of Defense, Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2016, Annual Report to Congress*, May 2016, 109, www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf.

61. John Mecklin, "Disarm and Modernize."

62. For an overview of Chinese nuclear forces, see Hans M. Kristensen and Robert S. Norris, "Chinese Nuclear Forces, 2015," FAS Nuclear Notebook, *Bulletin of the Atomic Scientists* 71, no. 4 (2015), http://bos.sagepub.com/content/71/4/77.full.pdf+html.

63. Previously, China had one *Xia*-class submarine that entered service in 1986 and is no longer considered operational.

64. John Mecklin, "Disarm and Modernize."

delivery vehicles.[65] The key hypersonic technologies that have received support from these funds are the Air Force conventional strike missile (CSM), the Defense Advanced Projects Agency (DARPA)/ Air Force hypersonic test vehicle-2 (HTV-2) program, and the Army advanced hypersonic weapon (AHW).[66]

Reports indicate that the Air Force was assigned the lead role in developing the long-range missile capability for CPGS in mid-2008.[67] The CSM was intended to be a land-based system that combines the Minotaur IV launch vehicle[68] with a hypersonic boost-glide vehicle to deliver conventional payloads at near-global ranges within minutes to hours of launch.[69,70] According to DoD officials, the program has not been given an official deployment date, since the research, development, and testing programs of hypersonic delivery platforms is ongoing. The decision as to which hypersonic vehicle to deploy will not be made until the systems under development have been tested successfully in five demonstration flights. This may not happen until the next decade depending on progress in the testing program.[71]

According to publically available sources, only two U.S. hypersonic vehicles have undergone flight testing, the HTV-2 and the AHW.[72] In April 2010, DoD conducted its first test of the HTV-2 hypersonic glide vehicle, launched on a modified configuration of the Minotaur IV rocket. According to DARPA, preliminary results showed that the HTV-2 achieved controlled flight in the atmosphere before telemetry was lost nine minutes after liftoff.[73] Media reports deemed the launch to be a partial success, noting that the boost mechanism performed a successful launch. The detachment

---

65. Amy Woolf, "Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues," Congressional Research Service, February 24, 2016, https://fas.org/sgp/crs/nuke/R41464.pdf.

66. The Air Force began an analysis of alternatives study in 2006 to review technologies and programs that could meet the requirements of the prompt global strike mission. Reports indicate that the Navy and Air Force collaborated on the study, exchanging information on service-specific platforms, and considering a range of alternative platforms, across service lines, for the long-term PGS option. These include a long-range land-based option, a shorter-range forward-deployed land-based missile, a sea-based option, and an air-breathing option. The Air Force completed this study in 2008. For more information see Elaine M. Grossman, "U.S. Military Eyes Fielding 'Prompt Global Strike' Weapon by 2015," Global Security Newswire, July 1, 2009, http://www.nti.org/gsn/article/us-military-eyes-fielding-prompt-global-strike-weapon-by-2015/.

67. Elaine M. Grossman, "Chilton Shifts Prompt Strike Priority to the Air Force," Global Security Newswire, September 3, 2008, http://www.nti.org/gsn/article/chilton-shifts-prompt-strike-priority-to-air-force/.

68. Grossman, "U.S. Military Eyes Fielding 'Prompt Global Strike' Weapon by 2015."

69. U.S. Department of Defense, *Fiscal Year 2011 Budget Estimates, Research Development, Test and Evaluation* (Washington, DC: Office of the Secretary of Defense, February 2010), 257, http://comptroller.defense.gov/defbudget/fy2011/budget_justification/pdfs/03_RDT_and_E/OSD%20RDTE_PB_2011_Volume%203B.pdf.

70. Major Jason E. Seyer, "Adding the Conventional Strike Missile to the US's Deterrence Toolkit," *High Frontier*, February 2009, http://www.thelivingmoon.com/91_PDF_Database/US_Space_Command/AFD-090224-115.pdf.

71. Elaine M. Grossman, "Cost to Test Global-Strike Missile Could Reach $500 Million," Global Security Newswire, March 15, 2010, http://www.nti.org/gsn/article/cost-to-test-us-global-strike-missile-could-reach-500-million/.

72. Ibid.

73. "Falcon HTV-2 Launch Test Hypersonic Vehicle Flight Capabilities," Fact Sheet, Defense Advanced Projects Agency (DARPA), Washington, DC, April 23, 2010, http://pop.h-cdn.co/assets/cm/15/06/54d15317917d2_-_FalconHTV-2FactSheet-1.pdf.

was also successful, though the glider itself failed to fly the full time and total distance. A second test of the HTV-2 vehicle in August 2011 exposed a flight anomaly post perigee that prompted the system to make a controlled descent and splash down in the ocean.[74] The combination of this poor test record and tight budget environment has undermined the future of this program. In fiscal year (FY) 2014, FY2015, and FY2016 budget requests, DoD sought only $2 million for this program area to conduct studies to evaluate system alternatives, and to continue aerodynamic risk reduction and technology maturation efforts.[75] DoD, however, does not plan to conduct additional flight tests of the HTV- 2.

DoD has since shifted efforts to the AHW boost-glide vehicle. The Army conducted a successful flight test of the AHW in November 2011,[76] using a booster stack derived from the Navy's Polaris ballistic missile. The Army conducted a second flight test in August 2014[77] during which the controllers destroyed the weapon after detecting problems with the booster four seconds after launch. Neither the booster nor the hypersonic vehicle contributed to the test's failure. As a result, DoD plans to move forward with the test program and has scheduled flights of a scaled version of the AHW for 2017 and 2019.

DARPA/Air Force is also funding a research development program, apart from CPGS, for the hypersonic air-breathing weapon concept (HAWC)[78] to develop and demonstrate critical technologies to enable an effective and affordable air-launched hypersonic cruise missile. This program intends to validate key technologies that could extend to future reusable hypersonic air platforms for applications such as intelligence, surveillance, and reconnaissance (ISR) and space access.

Hypersonic glide, boost-glide, and air-breathing vehicles are intended to play a niche role in the U.S. conventional strike capability. The George W. Bush administration initiated the CPGS program to develop fast, long-range, nonnuclear weapons capable of striking targets anywhere in the world in one hour or less.[79] According to James Acton, the mission objectives of the CPGS

74. "DARPA Hypersonic Vehicle Splash Down Confirmed," Defense Advanced Research Projects Agency (DARPA), Washington, DC, August 14, 2011, http://www.darpa.mil/NewsEvents/Releases/2011/2011/09/11_darpa_hypersonic_vehicle_splash_down_confirmed.aspx.

75. Amy Woolf, "Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues," Congressional Research Service, February 24, 2016, https://fas.org/sgp/crs/nuke/R41464.pdf.

76. Ann Roosevelt, "First Test Flight Successful for Advanced Hypersonic Weapon Vehicle," *Defense Daily*, November 18, 2011, 6.

77. Colin Clark, "Hypersonic Weapons Face Major Milestone in August Test," *Breaking Defense*, March 18, 2014, http://breakingdefense.com/2014/03/hypersonic-weapons-face-major-milestone-in-august-test/.

78. Mark Gustafson, "Hypersonic Air-Breathing Weapon Concept," Defense Advanced Projects Agency (DARPA), Washington, DC, date accessed April 9, 2016, http://www.darpa.mil/program/hypersonic-air-breathing-weapon-concept.

79. Keith Payne, "Conventional Prompt Global Strike: A Fresh Perspective," National Institute for Public Policy, June 2012, http://www.nipp.org/wp-content/uploads/2015/11/CPGS_REPORT-for-web.pdf. According to some strategic military targeteers, Prompt Global Strike weapons may be able to destroy 30 percent of the targets traditionally held at risk by nuclear weapons with conventional precision-strike missiles. Hans Kristensen, "Talks at U.S. Strategic Command and University of California San Diego," Federation of American Scientists, August 12, 2012, http://fas.org/blogs/security/2012/08/talks/.

Table 1. Features of the Russian, Chinese, and U.S. Hypersonic Glide, Boost-Glide, and Air-Breathing Vehicle Programs

Country	Vehicle Name	Launch Platform	Engine / Fuel	Test Rate	Test Efficacy
Russia	Yu-71 / 3M22 Zircon	SS-19 / UR-100N	Two-stage / liquid fuel	2010–2016, 5 tests	1 successful test of 5
People's Republic of China	DF-ZF / Wu-14	DF-11, -15, -16, -21, -26 variants	Single or two-stage / solid fuel	2014–2016, 7 tests	6 successful tests of 7
United States	HTV-2 AHW HAWC	Minotaur IV / Polaris	Scramjet / JP-7 fuel	2010–2014, 4 tests	1 successful test of 4

Note: AHW, advanced hypersonic weapon; HAWC, hypersonic air-breathing weapon concept.

program are to deny emerging nuclear proliferants the ability to employ nuclear arsenals; destroy or disable anti-satellite capabilities; counter anti-access/area-denial capabilities; and kill high-value terrorists and disrupt terrorist operations.[80] He notes that the degree of maneuverability and evasiveness varies for each mission objective.[81] The pursuit of hypersonic glide, boost-glide, and air-breathing vehicles provide a range of potential future capabilities for the United States.

The development of hypersonic glide, boost-glide, and air-breathing vehicles is not an aspect of U.S. nuclear modernization efforts. In fact, since its inception, the CPGS program has limited the design and technical specifications of hypersonic prototypes to outfit only conventional weapons. Moreover, introducing a new nuclear delivery platform is not currently in alignment with the strategy, policies, or agreed-upon budgets for the current 25-year nuclear modernization effort, and would not be feasible without concerted executive and legislative support to respond to what is now clearly a manifestly different strategic environment. The Obama administration implemented policies and initiatives to reduce the size and scope of the U.S. nuclear arsenal. In 2011, the Obama administration signed the New Strategic Arms Reduction Treaty (New START), authorizing the reduction of the total number of deployed nuclear weapons to 1,550.[82] Furthermore, in 2014, the Obama administration proposed and informally enacted the 3+2 strategy to decrease the diversity of nuclear weapons types from seven to five.[83] Under this strategy, the Department of

80. Acton, "Silver Bullet."

81. Ibid.

82. "New START," U.S. Department of State, accessed September 1, 2016, http://www.state.gov/t/avc/newstart/index.htm.

83. "Fiscal Year 2014 Stockpile Stewardship and Management Plan Report to Congress," U.S. Department of Energy, June 2013, http://nnsa.energy.gov/sites/default/files/nnsa/06-13-inlinefiles/FY14SSMP_2.pdf.

Energy/National Nuclear Security Administration (DOE/NNSA) has been given the responsibility to decrease the types of nuclear weapons and refurbish the selected weapons against the effects of aging,[84] while the DoD modernizes compatible nuclear delivery platforms that have been operational for decades. These refurbishment and modernization plans do not introduce new capabilities for nuclear weapons systems. It can be argued that the current U.S. decision not to design and test hypersonic vehicles capable of carrying nuclear explosives, choosing instead to refurbish older weapons certified for and delivered by traditional platforms, has the potential to create a significant strategic imbalance over time that will not favor U.S. security interests.[85]

WHY ARE RUSSIA AND CHINA DEVELOPING NUCLEAR CAPABLE HYPERSONIC DELIVERY SYSTEMS?

Russia and China's consternation over the development and forward deployment of U.S. antiballistic missile defense systems, its ongoing hypersonic vehicle development, and nuclear modernization program appear to be driving a series of strategic countermoves that must be taken into account by U.S. policymakers responsible for ensuring long-term U.S security. Russia and China continue to view the U.S. antiballistic missile defense systems as problematic for international strategic nuclear stability, and view the forward deployment of antiballistic missile defense systems as a type of containment or encirclement policy aimed at Russia and China.[86] The next section describes various strategic concerns driving Russian and Chinese hypersonic development activities and nuclear armament calculus.

Cancellation of the Anti-Ballistic Missile Treaty and the Rise of U.S. Ballistic Missile Defense Initiatives

U.S. hypersonic development was intended to prevent rogue states and non-state actors from obtaining weapons of mass destruction.[87] According to Kim Holmes, in the wake of September 11, 2001, ballistic missile technology was proliferating at such an alarming rate that the Bush

84. The implementation of the 3+2 strategy requires unparalleled diagnostic equipment to evaluate nuclear weapon aging, cutting-edge modeling, and simulation capabilities to examine what might happen if existing components are refurbished, and an exceptional cross-cutting workforce able to analyze and implement the results. The expected total cost of implementing the 3+2 strategy is $350 billion.

85. Furthermore, estimates on refurbishment costs continue to rise, leaving open the possibility, as a matter of public policy, that it may be more cost-effective to fabricate new explosives on a more regular basis with shorter expected lifetime cycles to address the evolving and dynamic strategic threat environment.

86. Emanuele Scimia, "China and Russia Concerned over America's Anti-Missile Moves," *Asia Times*, August 16, 2016, http://atimes.com/2016/08/china-and-russia-gripped-by-the-us-anti-missile-moves/.

87. Eleni Ekmektsioglou, "Hypersonic Weapons and Escalation Control in East Asia," *Strategic Studies Quarterly* 9, no. 2 (Summer 2015), http://www.au.af.mil/au/ssq/digital/pdf/summer_2015/SSQ_Summer_2015.pdf; Steven Pifer and James Tyson, *Third-Country Nuclear Forces and Possible Measures for Multilateral Arms Control*, Arms Control and Non-Proliferation Series Paper 12 (Washington, DC: Brookings Institutions, August 2016), https://www.brookings.edu/wp-content/uploads/2016/08/acnpi_20160824_multilateral_arms_control_01.pdf.

administration did not want to leave Americans vulnerable.[88] Given the existing geopolitical climate, the Bush administration decided it was becoming increasingly probable that non-state actors and rogue nation-states were planning to develop missile delivery systems for weapons of mass destruction; therefore, in addition to hypersonic strike capabilities designed to target rogue states by conventional means, defensive antiballistic missile measures were also necessary. The U.S. antiballistic missile defense system was intended to protect the United States against potential missile threats from rogue states and non-state actors by deploying a limited ballistic missile defense system.[89] However, to field this type of system legally, the United States needed to opt out of its long-standing Anti-Ballistic Missile (ABM) Treaty with Russia, which prohibited the deployment of national missile defense systems against long-range ballistic missiles.[90] The United States attempted to assure Russia that any decision to withdraw from the treaty and to create an antiballistic missile defense system was not targeted toward Russian strategic capabilities, but instead was meant to deal with increasingly unstable rogue nation-states and non-state actors who were pursuing nuclear weapons and ballistic missile strike capabilities of their own. In light of the U.S. security concerns described above, the United States elected to withdraw from the ABM Treaty in 2002, ending the 40-year agreement with Russia.[91]

Since the treaty withdrawal in 2002, the United States has allocated roughly $100 billion in funding to advance land- and sea-based antiballistic missile defenses (2002–2014 figures).[92] Today, the United States has four deployed missile defense architectures: the PATRIOT family of interceptors for point defense against shorter-range threats; the terminal high-altitude area defense (THAAD) for larger area defense; the ground-based midcourse defense (GMD) to defend the homeland; and the ship-based missile defense system, Aegis, employing the standard missile-3 (SM-3) to provide fleet and regional defenses against short-, medium-, and intermediate-range threats.[93]

---

88. Kim Holmes, "The 10th Anniversary of the Anti-Ballistic Missile Defense Treaty Withdrawal," Heritage Foundation (Lecture #1220 on Arms Control and Nonproliferation), February 14, 2013, http://www.heritage.org/research/lecture/2013/02/the-10th-anniversary-of-the-anti-ballistic-missile-treaty-withdrawal.

89. Nathan Voegeli, "A Look at National Missile Defense and the Ground-Based Midcourse Defense System," Nuclear Threat Initiative, 2005, http://www.nti.org/analysis/articles/look-national-missile-defense/.

90. Wade Boese, "U.S. Withdraws from ABM Treaty; Global Response Muted," Arms Control Association, July 1, 2002, https://www.armscontrol.org/act/2002_07-08/abmjul_aug02.

91. Ibid.

92. Ibid. Also see Jonathan Masters, "Ballistic Missile Defense," Council on Foreign Relations, August 15, 2014, http://www.cfr.org/missile-defense/ballistic-missile-defense/p30607. The first ground-based missile interceptor was installed at an army base in central Alaska in July 2004. By February 2007, the U.S. missile defense system consisted of 13 ground-based interceptors in Alaska and 2 ground-based interceptors in California, with a plan to increase to 21 interceptors by the end of 2007. This spending resulted in initial deployment of anti-ballistic missile technologies, although the efficacy of these systems remains an open question. For more information see Steven Pifer, "The Limits of U.S. Missile Defense," Brookings Institution, March 30, 2015, https://www.brookings.edu/opinions/the-limits-of-u-s-missile-defense/.

93. Kiron Skinner, "Missile Defense: Past Present, and Future," *Strategika: Conflicts of the Past as Lessons for the Present*, no. 27, October 2015, http://www.hoover.org/sites/default/files/issues/resources/strategika_issue_27_web.pdf.

Recent placement of U.S. missile defense architectures in Eastern Europe, and announcements to place additional architectures in the Asia Pacific, point toward a strategic shift in signaling with the employment of the U.S. antiballistic missile defense system, which has alarmed Russia and China. The United States has extended protection to U.S. allies by placing antiballistic missile defense systems on foreign soil. In May 2016, after a decade of trilateral public announcements and planning,[94] the United States deployed a ground-based missile defense system in Romania[95] and broke ground on the future site of an Aegis Ashore ballistic missile defense system in Poland.[96] Both systems, which will be operated by the North Atlantic Treaty Organization (NATO), are considered necessary to defend U.S. allies in Eastern Europe against rogue nation-states, most notably Iran.[97] Additionally, in July 2016, after months of bilateral deliberation, the United States announced the future deployment of a THAAD system in South Korea to shield its ally from North Korea's intensifying missile threats.[98]

Russia's Perspective

At the St. Petersburg International Economic Forum in 2015, President Vladimir Putin declared that the U.S. abrogation of the ABM Treaty and successive actions have pushed the world to a new Cold War; moreover, it pushed Russia to a new round of the arms race by altering the global security paradigm.[99] Moscow perceives the U.S. withdrawal from the treaty, development of an antiballistic missile defense system, its ongoing technological advancements to develop a new offensive hypersonic weapon, and forward deployment of two defense architectures to Eastern Europe as aimed at blunting Russia's nuclear arsenal and imperiling its security.[100] Russian fears can be traced to its vocal opposition to the U.S. withdrawal from the ABM Treaty. In 2001, President Putin announced that the U.S. withdrawal from the ABM Treaty was an "erroneous" decision,[101] as

94. Soraya Sarhaddi Nelson, "U.S. Enlarges Its Military Footprint in Eastern Europe, to Mixed Reviews," National Public Radio, May 18, 2016, http://www.npr.org/sections/parallels/2016/05/18/478414178/u-s-enlarges-its-military-footprint-in-eastern-europe-to-mixed-reviews.

95. Ryan Browne, "U.S. Launched Long-Awaited European Missile Defense Shield," CNN, May 12, 2016, http://www.cnn.com/2016/05/11/politics/nato-missile-defense-romania-poland/.

96. Lisa Ferdinando, "Work Joins Groundbreaking for Ballistic Missile Defense Site in Poland," U.S. Department of Defense, May 13, 2016, http://www.defense.gov/News/Article/Article/759662/work-joins-groundbreaking-for-ballistic-missile-defense-site-in-poland.

97. Robin Emmott, "U.S. Activates Romanian Missile Defense Site, Angering Russia," Reuters, May 12, 2016, http://www.reuters.com/article/us-nato-shield-idUSKCN0Y30JX.

98. Scott Snyder, "China's Limited Retaliation Options against the THAAD Deployment in South Korea," *Forbes*, August 9, 2016, http://www.forbes.com/sites/scottasnyder/2016/08/09/chinas-limited-retaliation-options-against-the-thaad-deployment-in-south-korea/#1f20347b7a98.

99. "Putin: Unilateral US Withdrawal from ABM Treaty Pushing Russia toward New Arms Race," *Russia Today*, June 19, 2015, https://www.rt.com/news/268345-putin-west-russia-relations/.

100. Andrew Kramer, "Russia Calls New U.S. Missile Defense System a 'Direct Threat,'" *New York Times*, May 12, 2016, http://www.nytimes.com/2016/05/13/world/europe/russia-nato-us-romania-missile-defense.html?_r=0.

101. Terence Neilan, "Bush Pulls Out of ABM Treaty; Putin Calls Move a Mistake," *New York Times*, December 13, 2001, http://www.nytimes.com/2001/12/13/international/bush-pulls-out-of-abm-treaty-putin-calls-move-a-mistake.html?_r=0.

the treaty was long regarded by Moscow as a cornerstone of strategic stability.[102] It was understood that if either the United States or Russia constructed a missile defense system, the other would build offensive nuclear forces to offset the defense.[103] The U.S. antiballistic missile defense expansion, the placement of a ground-based missile defense system in Romania and forthcoming Aegis ballistic missile defense system in Poland, reinforces Moscow's perception of a concerted U.S. military and political containment strategy focused on Russia.[104] The continued plans for deployment of these two systems—even after a successful nuclear deal with Iran was consummated,[105] which should ostensibly obviate the need for these protective measures—is reportedly seen as proof that the United States and NATO have ulterior motives.[106] These motives, according to the Russian narrative, may include assisting Eastern European neighbors with the development of their own missile defense systems and integrating them into the broader U.S. antiballistic missile defense umbrella.[107]

The announcement and imminent deployment of a ground-based missile defense and an Aegis in two NATO-aligned countries surrounding Russia seemingly acted as an impetus for expediting the timeline of Russian countermoves, including hypersonic and nuclear modernization development.[108] In 2014, Russia's Deputy Prime Minister Dmitry Rogozin announced a military reprioritization to field a nuclear hypersonic glide vehicle, as well as a substantial inventory of tactical nuclear weapons, nuclear weapons–carrying platforms, and an increasing inventory of theater-range tactical nuclear technologies.[109] In the final analysis, it seems that Moscow believes that the coupled deployment of the U.S. antiballistic missile defense system and development of hypersonic technologies increases the potential for a successful U.S. preemptive strike against Russian nuclear missiles.[110]

---

102. Pavel Podvig, "Missile Defense and the Myth of Strategic Stability," Russian Forces (presentation for Stability Issues in a New Nuclear Order workshop, Berlin, December 15–16, 2014, http://russianforces.org/podvig/Podvig-Missile%20defense%20and%20strategic%20stability.pdf.

103. Wade Boese, "U.S. Withdraws from ABM Treaty; Global Response Muted," Arms Control Association, July 1, 2002, https://www.armscontrol.org/act/2002_07-08/abmjul_aug02.

104. Kyle Mizokami, "Russia Is Not Happy about New American Anti-Ballistic Missile System," *Popular Mechanics*, May 16, 2016, http://www.popularmechanics.com/military/weapons/a20902/russias-unhappy-about-new-american-anti-missile-system/.

105. Judah Ari Gross, "8 Iranian Missile Launches since Nuke Deal Signed, Expert Tells US Congress," *Times of Israel*, May 26, 2016, http://www.timesofisrael.com/8-iranian-missile-launches-since-nuke-deal-signed-expert-tells-us-congress/. While a joint comprehensive plan of action intends to curtail Iranian nuclear warhead development, no agreement has successfully halted Iran's continued nuclear missile development and test launches.

106. Ibid.

107. Scimia, "China and Russia Concerned over America's Anti-Missile Moves."

108. According to Col. Gen. Vladimir Yakovlev, former commander-in-chief of the Russian strategic missile force, Russia considered the countermeasures it would take in the wake of the U.S. withdrawal from the ABM Treaty and implemented steps to realize those countermeasures. Nikolai Novichkov, "Russia's Warning on Treaty Violations," *Jane's Defence Weekly*, October 27, 1999.

109. Shapiro, "Russia Launching New Hypersonic Missile to Carry Nuclear Warheads."

110. Richard Weitz, "Global Insights: Common Fears, Different Approaches to U.S. BMD [ballistic missile defense] for Russia, China," *World Politics Review*, November 27, 2012, http://www.worldpoliticsreview.com/articles/12524/global-insights-common-fears-different-approaches-to-u-s-bmd-for-russia-china.

China's Perspective

Beijing suspects that the United States has developed missile defenses capable of negating China's strategic nuclear deterrent since its withdrawal from the ABM Treaty,[111] and views the U.S. decision to place antiballistic missile defense systems in the Asia Pacific as supportive evidence. China assesses that the U.S. antiballistic missile defense system includes at least one radar with a range extending far beyond the Korean peninsula into Chinese territory, giving the United States the potential to track China's military capabilities,[112] thus threatening China's deterrence force and its regional balance of power.[113] The placement of a U.S. antiballistic missile defense system in the Asia Pacific is argued to worsen the regional security environment.[114] Beijing perceives itself as an emerging player in the long-established bi-polar world of nuclear weapons, and believes that moves made by the United States are intended to stymie the growth of China's nuclear weapons arsenal, thereby impacting its standing in the regional and international community.[115]

China shares the Russian view that the forward deployments of U.S. antiballistic missile defense systems are a type of containment or encirclement policy.[116] China warns that U.S. antiballistic missile defense systems will break global strategic balance and stability, will obstruct the process of nuclear disarmament and nonproliferation, and may even trigger a new round of arms races.[117] China continues to intensify its response to the antiballistic missile defense system by modernizing its strategic forces, increasing their mobility and numbers while improving the survivability of reentry vehicles.[118] Although the exact size of China's nuclear stockpile has not been publicly disclosed, the Union of Concerned Scientists reports that as of 2011 China has produced a total of 200 to 300 nuclear warheads.[119] In 2015, Kristensen and Norris estimated the size of China's current nuclear stockpile to be approximately 260 warheads and slowly increasing.[120] The

---

111. Richard Weitz, "China Steps up Rhetoric against U.S. Missile Defense," *China Brief* 12, no. 20 (October 19, 2012), http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=39996&cHash=36d0c53bbdb14799e970e6a6c0593911.

112. Alex Gorka, "US to Deploy BMD System in South Korea," Strategic Culture Foundation, July 10, 2016, http://www.strategic-culture.org/news/2016/07/10/us-deploy-bmd-system-south-korea.html.

113. Ibid.

114. Chen Zhou, "Anti-Ballistic Missile Program: Does No Good to World Peace and Security," China-US Focus, August 24, 2012, http://www.chinausfocus.com/peace-security/anti-ballistic-missile-program-does-no-good-to-world-peace-and-security/.

115. Ibid.

116. Weitz, "China Steps up Rhetoric against U.S. Missile Defense"; U.S. Department of Defense, *Ballistic Missile Defense Review Report*, February 2010, http://archive.defense.gov/bmdr/docs/BMDR%20as%20of%2026JAN10%200630_for%20web.pdf.

117. Chen Zhou, "Anti-Ballistic Missile Program."

118. Tom Collina, "Dumping the ABM Treaty: Was It Worth It?," Arms Control Now, July 12, 2012, https://armscontrolnow.org/2012/06/12/2969/.

119. Gregory Kulacki, "China's Nuclear Arsenal: Status and Evolution," Union of Concerned Scientists, October 2011, http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/UCS-Chinese-nuclear-modernization.pdf.

120. Kristensen and Norris, "Chinese Nuclear Forces, 2015."

Stockholm Peace Institute believes that roughly 190 of these warheads can currently be considered operational.[121] The imminent deployment of hypersonic boost-glide vehicles may increase the number of nuclear warheads in China's stockpile while providing a new offensive capability to upset the current paradigm of nuclear stability.

ANALYSIS

The U.S. withdrawal from the ABM Treaty, coupled with the establishment of the CPGS program and antiballistic missile defense system, has likely created an unintended defensive spiral with Russia and China. The Bush administration made a series of unilateral decisions in the wake of the September 11, 2001, attacks to employ additional security measures to protect U.S. citizens against actual and perceived threats from non-state actors and rogue nation-states. Although the Bush administration's decisions were justifiable at the time they were enacted, they can be viewed as disproportionate to the threat by the time they were employed, resulting in potentially grave consequences for U.S. security interests in light of Russian and Chinese countermoves. The development of hypersonic vehicles, coupled with the development and forward deployment of U.S. antiballistic missile defense systems, upset a long-established strategic balance with Russia and China, not only through the pursuit of an advanced, albeit conventionally armed first-strike capability, but also by creating the potential, if not the capability, to undermine Russia and China's belief in their assured second-strike capabilities.

Russia and China believe that U.S. decisions on the ABM Treaty, CPGS, and antiballistic missile defense created a strategic nuclear imbalance that has upended global stability. Their argument, whether reasonable or not, has driven their development and potential deployment of dual-capable hypersonic weapons, an equally destabilizing set of strategic countermoves. Because hypersonic weapons can be used for both preemptive and retaliatory purposes, their potential deployment is on track to create a continuing strategic imbalance—this time, in favor of Russia and China. It is reasonable to deduce that the United States, or countries reliant upon the U.S. antiballistic missile systems in Eastern Europe and the Asia Pacific, may be targeted by these dual-capable systems as a next step in the defensive spiral. Potential objectives could be to destroy nuclear silos and submarines; command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems; production and storage facilities; high-value personnel; and anti-satellite and anti-access/area-denial capabilities. Regardless of the configuration, the United States and U.S. allies are arguably more at risk now that this defensive spiral paradigm has been established.

If the U.S. objective is to sustain strategic nuclear stability and continue to support a reasonable level of assured strategic balance with Russia and China, U.S. decisionmakers must weigh potential options to ensure the maintenance of an equal footing with Russian and Chinese nuclear forces in the coming years. In light of their technological advancements, this strategy must include initiatives sufficient to dissuade any inclinations these countries might have to actually use nuclear

121. "Military Spending and Armaments, Nuclear Forces: China," Stockholm International Peace Research Institute, 2014, https://www.sipri.org/research/armaments-and-disarmament/nuclear-weapons/world-nuclear-forces/china.

armed hypersonic delivery systems as an overwhelming first-strike capability. Verbal assurances to Russia and China regarding U.S. intent related to hypersonic platform research and development and antiballistic missile defense deployments have proven ineffective. Fortunately, an opportunity exists to formulate a revised U.S. nuclear weapons and countermeasures strategy and express U.S. strategic intent and policy in the 2017 Nuclear Posture Review. The following section provides possible courses of action that may be considered.

POSSIBLE COURSES OF ACTION FOR U.S. DECISIONMAKERS

1. The United States can increase its level of effort for hypersonic development and modify the scope of work to include the exploration of dual-capable hypersonic platforms to hold adversaries equally at risk. This would require a change to U.S. policy regarding nuclear modernization.

The 2010 Nuclear Posture Review published by the DoD did not account for hypersonic glide, boost-glide, or air-breathing vehicles, perhaps because it assessed that the maturation of this technology was far off into the future as not to constitute an emerging threat, in part due to the considerable technological challenges of achieving and sustaining flight at hypersonic speeds and low trajectories. Today's reality would require an acknowledgment that Russian and Chinese nuclear-armed hypersonic weapons are a very real and rapidly emerging threat to U.S. national security. The 2017 Nuclear Posture Review would be an appropriate forum for U.S. policymakers to begin reassessing hypersonic platform development and properly inform the establishment of a future congressional program of record.

DoD is currently planning a replacement ICBM capability with a total program cost projected to be $62 billion from FY2015 through FY2044.[122] Specifically, the DoD is working to replace the Boeing LGM-30G Minuteman III ICBM with the ground-based strategic deterrent (GBSD), in order to maintain a similar land-based deterrent capability the United States has exercised for 45 years. The program cost breaks down to about $14 billion for upgrades to command-and-control systems and launch centers, and $48.5 billion for replacement missiles.[123] While assuring a delivery capability for this element of the nuclear triad is essential, it may not be sufficient. The planned future capabilities of near-peer countries may undermine the efficacy of a one-for-one capability replacement of the Boeing LGM-30G Minuteman III ICBM, and therefore the technical approach for this newly announced system must be continually examined to determine the efficacy of this element of nuclear deterrent. For good or ill, hypersonic glide, boost-glide, and air-breathing vehicles provide an asymmetric advantage over ICBMs. According to all the reports cited in this paper, they are more maneuverable weapons that can bypass existing antiballistic missile defenses and hit specific targets with what can only be imagined as pinpoint accuracy when fully operationalized. As an emerging technology, the advantages of hypersonic glide, boost-glide, and

122. Stew Magnuson, "Air Force Kicks Off Program to Replace Minuteman III Missiles," *National Defense*, August 2016, http://www.nationaldefensemagazine.org/archive/2016/august/Pages/AirForceKicksOffProgramtoReplaceMinutemanIIIMissiles.aspx.

123. DoD Future Years Defense Program (FYDP) 2016–2020 for the GBSD, Defense Technical Information Center, February 2015, http://www.dtic.mil/descriptivesum/Y2016/AirForce/0605230F_4_PB_2016.pdf.

air-breathing vehicles are potentially so great that one-for-one capability replacements of ICBMs may become less effective in the triad over time, unless they incorporate a modular design approach to accommodate additional capabilities such as maneuverability and precision strike, and consider the possible insertion of hypersonic weapons, which may require additional research prior to system acquisition. The year 2017 may be the appropriate time to adjust investment priorities to bolster hypersonic research and development projects to explore the technical feasibility of hypersonic maneuverable ICBMs, while fast-tracking the operational deployment of hypersonic glide, boost-glide, and air-breathing vehicles in the CPGS portfolio.

Policymakers may want to consider accelerating the rapid development of hypersonic delivery vehicle maturation and testing to create an operationally deployable system by 2025. In the 13 years since the inception of the CPGS program, the total program cost has been $986 million, an approximate average of $76 million per year. Amy Woolf noted the size of the CPGS portfolio indicates that the DoD is focused primarily on the feasibility of the technology.[124] Stephen Welby reaffirmed that the U.S. hypersonic glide, boost-glide, and air-breathing vehicle programs are purely technology development programs.[125] In light of near-peer capability demonstrations and testing rates, this technology gap clearly needs to be addressed as a priority.

However, increasing the level of funding without changing the scope of work will not stabilize nuclear deterrence. If Russia and China develop and deploy hypersonic glide and boost-glide vehicles in nuclear as well as conventional configurations, the United States will most likely be at a disadvantage if it elects to create only conventional configurations. In order to maximize the efficacy of the investment in this technology, a change in scope and a change in policy must also occur alongside an increase in funding. The United States would need to broaden its nuclear modernization portfolio to account for the use of hypersonic delivery vehicles for nuclear explosives. As a matter of policy, accounting for the possibility of placing nuclear explosives on hypersonic glide, boost-glide, and air-breathing vehicles, at a minimum, allows the U.S. defense establishment the flexibility to pursue symmetric capabilities as warranted by near-peer program initiatives and deployments. It would seem prudent that the United States explore the technical feasibility of dual-capable hypersonic platforms as soon as possible, thus continuing to ensure an acceptable level of nuclear deterrence exists among the three countries.

2. The United States can develop countermeasures for hypersonic glide, boost-glide, and air-breathing weapons. Some possibilities that have been proffered are hit-to-kill improvements, directed energy advancements, and asymmetric warfare tactics.

The United States should advance its antiballistic missile defense systems to account for hypersonic glide, boost-glide, and air-breathing hypersonic weapons. The existing U.S. antiballistic missile defense system reportedly cannot defend against hypersonic weapons. Dean Wilkening stated that a number of the deployed missile defense architectures are essentially prototype

124. Woolf, "Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues."

125. Patrick Tucker, "The Problem with the Pentagon's Hypersonic Missile," April 14, 2016, http://www.defenseone.com/technology/2016/04/problem-pentagon-hypersonic-missile/127493/.

designs.[126] Redesigns scheduled in the next 15 years will be operationally more effective.[127] He predicts that the United States will remain dependent on hit-to-kill interceptor technologies, with the largest measurable improvements being operational consistency.[128]

Ongoing research and development into new missile defense designs and applications may eventually provide ancillary value to hit-to-kill interceptors. John Stillion assessed that directed energy sources will eventually bolster U.S. antiballistic missile defenses.[129] Wilkening has postulated that directed energy technologies have niche applications for point defense of military ships or bases;[130] however, it is unlikely that directed energy would be an effective defensive capability against hypersonic glide, boost-glide, or air-breathing vehicles.[131] Directed energy laser targeting systems would have to locate the target before it can fire and, afterwards, hold the beam on a precise point long enough to burn a hole into the delivery system. This technology may be insufficient for interdicting hypersonic vehicles that possess evasive maneuverability.

Possible future efficacy of electromagnetic railgun technology may provide a defense against hypersonic weapons. Electromagnetic railguns fire projectiles at Mach 6 using electricity instead of chemical propellants.[132] According to the Office of Naval Research, the increased velocity and extended range of an electromagnetic railgun may support precise naval surface fire or land strikes, ship defense, and surface warfare to deter enemy vessels.[133] A future version of this weapon system using high energy levels may be capable of launching a 100+ nautical mile projectile.[134] This launch energy has the advantage of being able to stress many components to evaluate full-scale mechanical and electromagnetic forces,[135] essentially frying the electronics of a reentry vehicle from within. Early warning and precision tracking would need to be coupled with the use of an electromagnetic railgun when aimed at hypersonic weapons, because railgun projectiles, like hit-to-kill interceptors and directed energy lasers, intercept a single point on a plane.

Theoretically, an effective defensive capability would need to protect a spatially multilayered area, and potentially exercise enhanced dimensionality and agility. A multi-constraints and multi-phase

---

126. Sydney Freedberg Jr., "The Limits of Lasers: Missile Defense at Speed of Light," Breaking Defense, May 30, 2014, http://breakingdefense.com/2014/05/the-limits-of-lasers-missile-defense-at-speed-of-light/.

127. Ibid.

128. Ibid.

129. Harry Kazianis, "The Real Military Game-Changer: Hypersonic Weapons 101," *Interpreter*, March 14, 2014, http://www.lowyinterpreter.org/post/2014/03/14/Hypersonic-weapons-101.aspx.

130. Sydney Freedberg Jr., "The Limits of Lasers: Missile Defense at Speed of Light."

131. Ibid.

132. "Electromagnetic Railgun Fact Sheet," Office of Naval Research Science and Technology, accessed September 7, 2016, http://www.onr.navy.mil/media-center/fact-sheets/electromagnetic-railgun.aspx.

133. Ibid.

134. Ibid.

135. Ibid.

trajectory optimization method should be considered to maximize reachable domain and minimize attack time.[136]

According to Harry Kazianis, the United States may need to consider other possible asymmetric warfare tactics, including electronic warfare, the use of jammers, or other electronic countermeasure techniques that could deny targeting data to the attacker or confuse the hypersonic vehicle's own sensors as it attempts to hit its target. Disrupting communication links between sensing, command-and-control, and missile units is another possible means of decreasing the effectiveness of such weapons.[137] Instead of focusing on point solutions to shoot down hypersonic weapons with hit-to-kill intercepts, directed energy lasers, or electromagnetic railguns, the United States could consider using a variety of techniques as part of an integrated defensive package.

3. The United States can promote the establishment of international norms for the development, deployment, and use of hypersonic missiles.

Generally speaking, engaging in Track II diplomacy with Russia and China may be the precursor to confidence-building measures necessary for the establishment of international norms for the development, deployment, and use of hypersonic vehicles, including the preclusion of nuclear armaments on these platforms. As a first step, unofficial collaborative technical exchanges might be explored to build relationships at the individual level and encourage new thinking that can inform the official process.[138] These types of exchanges are typically a precursor to breaking long-established, and often perpetuated, distrust at the national level.

Demonstrated success with collaborative technical exchanges and Track II diplomacy might lead to bilateral or multilateral employment of confidence-building measures designed to reduce the level of fear among the parties. Russian and Chinese officials have expressed concerns that U.S. missile defenses adversely affect their own strategic capabilities and interests. Both have reportedly pursued hypersonic technologies because of their ability to evade U.S. antiballistic missile defenses. The United States might consider continuing bilateral or multilateral exchanges with Russia and China to underscore the stated purpose of U.S. antiballistic missile defense systems, which are intended to protect the United States and its allies against perceived threats from rogue nation-states and non-state actors. Additionally, advanced bilateral or multilateral notification alerts for exercises, mobilization drills, and defensive maneuvers may subdue fears and reduce tensions regarding hypersonic weapon targeting by any or all nations involved, regardless of whether the vehicles are armed with conventional or nuclear explosives now or in the future.

---

136. Yu Li and Nai-gang Cul, "Optimal Attack Trajectory for Hypersonic Boost-Glide Missile in Maximum Reachable Domain," International Conference on Mechatronics and Automation, Changchun, China, August 9–12, 2009, http://ieeexplore.ieee.org/document/5246695/.

137. Kazianis, "The Real Military Game-Changer."

138. For more information on Track I and Track II diplomacy, see "What is Multi-Track Diplomacy?," Institute of Multi-Track Diplomacy, accessed September 4, 2016, http://imtd.org/multi-track-diplomacy.

Reduction in tensions and uncertainty may lay the foundation for Track I diplomatic negotiations of international norms with monitoring and verification mechanisms. International norms may include halting the research of hypersonic technology after reaching a specified point in the development cycle, precluding the use of nuclear armaments on these platforms, and/or limiting usability to a specified kilometer range in a specified scenario to avoid global conflict. This approach could facilitate the development of hypersonic technology as a new frontier in aerodynamics that clearly has a research value extending beyond weaponization to a range of civilian and space applications. The exploration of beneficial hypersonic technology applications requires the coupling of modeling, ground tests, and flight testing that could be matured through unofficial and later, formal, collaborative technical exchanges between subject matter experts in the United States, Russia, and China.

Regardless of the international norms agreed upon by the parties, it has been proven time and again through the Strategic Arms Limitations Treaties (SALT I, II, and III) and the New Strategic Arms Reduction Treaty (New START), among others, that treaty effectiveness depends, in part, upon the monitoring and verification mechanisms implemented. Measures have included on-site inspections and exhibitions, data exchanges and notifications related to strategic offensive arms and facilities, and provisions to facilitate the use of national technical means for treaty monitoring. Adopting a proven and effective model for establishing an international norm, which includes detailed reciprocal inspections to help stabilize the current geopolitical climate, may be a viable path for mitigating the threat posed by the development and deployment of militaristic hypersonic applications.

Engaging in Track II diplomacy, enacting confidence-building measures, and establishing international norms with effective tracking and verification mechanisms on these issues may, over time, ensure a less destabilizing international environment.

CONCLUSION

Although international norms for militaristic hypersonic applications may one day be viewed as an achievable ideal, based on the current international climate, and countermoves already made by Russia and China, the United States must plan for a potential strategic imbalance in the near term. The continued Russian and Chinese refinement of hypersonic glide and boost-glide technology, coupled with their stated intentions of placing nuclear armaments on those platforms, will create an untenable security situation for the United States if no countermanding action is taken. The 2017 Nuclear Posture Review would be an appropriate forum for U.S. policymakers to reexamine the assumptions and limitations of the current approach taken in the 3+2 strategy and to reassess the role of hypersonic weapons in the nuclear deterrent, including potential insertion into GBSD. As part of that review, it might well be reasonable to reconsider the current policy prohibiting the placement of nuclear weapons on hypersonic vehicles. In parallel to developing a comprehensive hypersonic strategic plan, the United States should continue its antiballistic missile defense systems advancements to include near-peer nuclear-armed hypersonic glide and boost-glide vehicles, while simultaneously engaging both Russia and China in the establishment of bilateral or

trilateral agreements to address and mitigate what is likely to become an iterative series of countermoves by all parties involved. Ideally, international norms with enforceable tracking and verification mechanisms can move the nations involved back into a level of acceptable strategic balance related to nuclear weapons, while accounting for cooperation against proliferant rogue nation-states and non-state actors seeking the ability to cause catastrophic nuclear weapons effects to advance their agendas.

COVER PHOTO U.S. AIR FORCE PHOTO BY STAFF SGT. JOCELYN RICH

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.**csis**.org

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

4501 Forbes Boulevard
Lanham, MD 20706
301 459 3366 | www.**rowman**.com