LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-833000

NSLP-Final Report-Draft2022

W. Dawson, J. Boles, K. Le Galloudec

March 22, 2022

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

A Method for Assessing Effectiveness and Technical Capabilities Required for Integrated Deterrence

Jeremiah Boles William Dawson Korbie Le Galloudec

Fall/Winter 2021

A report developed in partial fulfillment of the requirements for the National Security Affairs Program within the Bush School of Government and Public Service at Texas A&M

Advisor: Jasen Castillo, Texas A&M

Sponsor: Sheryl Hingorani, Lawrence Livermore National Laboratory

LLNL-TR-833000

Disclaimer

Lawrence Livermore National Laboratory is operated by Lawrence Livermore National Security, LLC, for the U.S. Department of Energy, National Nuclear Security Administration under Contract DE-AC52-07NA27344.

Executive Summary

The United States faces an ever-increasingly multi-polar security environment dominated by great power competition with China and a lingering Russian threat as well as from would-be regional hegemons led by ambitions from Iran and North Korea. Our adversaries are pursuing and expanding the strategic means by-which they have an asymmetric offset (e.g., cyber, space, and other modes below the level of armed conflict). To combat and deter against the widening range of hostile actions, the U.S. must have additional capabilities with-which to deter. All of which drives us towards a more thoughtful integrated approach to deterrence, attempting to best align deterrent tools with the adversary actions in order to maximize the credibility of our deterrent. Such an approach complicates our deterrence strategy and demands a methodology to assess whether the U.S. has the deterrent tools necessary to deter the adversarial actions most costly to the U.S.

To address this complexity, we create a framework to comprehensively and systematically assess our deterrent tools as qualitatively measured against the adversarial actions we wish to deter. Deterrence is ultimately an operation in the cognitive domain and at the heart of the framework presented here is the fundamental deterrence calculus which we use as the defining measure of whether a tool will credibly deter a given action. We describe the eight levers of the deterrence calculus and distill these levers to four products that are used to qualitatively assess the overall effectiveness of deterrence tools against adversarial actions. Credibility is determined by two principal variables: the technical credibility of the deterrent tool, and the principle of proportionality. Technical credibility of realized deterrence products is assessed through development of key mission requirements and hardware (e.g., components) that will impose costs, deny benefits, or encourage restraint. The principle of proportionality qualitatively asserts that for a deterrent tool to be cognitively credible, the costs imposed against, or benefits denied by, an action are commensurate to the magnitude of costs received from the adversarial action. By basing this framework on these two fundamentals, it is possible to compare deterrent tools in a systematic approach across the broad spectrum of hostile actions.

A complete analysis of all possible U.S. deterrence tools is beyond the scope of the current project. Therefore, we demonstrate the approach with a case study by first considering *what adversary actions are our nuclear weapons are good at deterring*, and second by conducting a more complete and informed, yet high-level, assessment of *how future science and technology might enhance or degrade our nuclear deterrent*. Note that the science and technology drivers will vary from 'deterrent tool'-to-'adversary action' pairing, thus a full systematic analysis like the one proposed here should be conducted before drawing concrete conclusions for at-large technical credibility assessments for other deterrence tools.

To answer the first consideration of what adversary actions our nuclear arsenal is good at deterring, we find that while the U.S. nuclear deterrent is technically capable of deterring a broad range of actions, it is limited by the principle of proportionality coupled with an often inflated perceived cost of nuclear weapons. We argue that nuclear weapons are typically only good at deterring other nuclear weapon attacks and questionable at being able to deter other forms of similarly costly attacks on the U.S. or its allies.

To understand and assess the second consideration for how science and technology might enhance or degrade the U.S. nuclear deterrent we have developed an analysis capability based on fundamental systems engineering and integration techniques. From this we perform a detailed science and technology focused assessment of the U.S. strategic nuclear arsenal to deter a massive nuclear first-strike on the U.S. homeland. Using this analysis capability, we identify high level technological capability drivers and gaps for each of the major hardware components of the Secure 2nd Strike deterrence tool where targeted efforts could be applied through our sponsor or other national efforts to enhance or mitigate degradation of the U.S. nuclear deterrent.

We find that warhead capabilities will be highly effective for long term needs, however, trends are negative due to inflexibility and production lead time for current lifecycle demands on warhead designs. We also find that delivery vehicles followed by nuclear command, control, and communications (NC3) are the sub-components at the highest risk of being disrupted by future science and technology developments.

In addition to the technical findings for the specific deterrence tool assessed herein, we find that in general, technological solutions are a necessary but double-edged sword, with frequent correlation between countervailing levers within the deterrence calculus. For example, increasing the technical ability to deter an adversary's action through threat of returned-cost imposition often increases the adversary's perceived need to act hostilely for fear of having a cost imposed on them if they don't act. In part this type of finding and influence within the deterrence calculus can and should be managed by the purveyors of technological solutions. It is also necessary to couple technical solutions with political solutions. Since much of the current U.S. deterrent credibility is limited by the principle of proportionality, and not technical capability, it would be in the best interest of the country to consider technical solutions in the context of the principle of proportionality in addition to their technical capability.

Through this report, we have provided a methodology and tool-kit for the development of capabilities, or tools, that will enable the assessment of specific deterrence capabilities to support a robust national defense strategy for the current strategic security environment. By matching threat actions to deterrence tools, future analysts can apply this methodology to assess the efficacy and proportionality of technical deterrence solutions relative to the threat actions to maximize and enhance the U.S. strategic deterrence capabilities. Furthermore, this tool-kit enables analysts to perceive insight into gaps within existing or postulated strategic deterrence capabilities. These insights can be used to trend ongoing research and development programs for comparison to the future effectiveness of a specific deterrence capability. By understanding the full scope of a deterrence tool, including both abilities and limitations, U.S. research laboratories, such as Lawrence Livermore National Laboratory, can effectively propose, develop, and prototype future deterrence capabilities to meet national security needs.

Table of Contents

Introduction

The state of the world continues to evolve and the challenges and risks to the United States have become more complex and interwoven. Our nation's leadership recognizes these changes and has indicated the need for a new approach in maintaining the security of our nation. Many of these changes are driven from the expansion of an interconnected world, starting after WWII with the Cold War and the rise of the liberal New World Order. Led by the U.S. and NATO, western-style democracies built an elaborate network of alliances and partnerships that engaged in economic and diplomatic trade. After the Cold War ended and the United States gained status as the global superpower, technical innovation flourished and created a revolution we see today as the information age. This period, over the last thirty years, is hallmarked by globalism, the state of international interdependency of trade, communications, industry, commerce, and capitalism.

However, many of the nations' enjoying prosperity brought about by current state of democratic affairs believe that they have equal standing with the United States and have thus created a multi-polar era where they can challenge U.S. supremacy in many sectors of the globe. This includes the return of great power competition as outlined in the 2017 National Security Strategy[1], the rise of cyber competition as outlined in the 2018 National Cyber Strategy[2], increased tensions from regional would-be hegemons[3], and expansion of interests counter to maintaining U.S.-led global world order[4]. These threats to U.S.-led order are in addition to the overt threats made by proliferant nations. North Korea and Iran have publicly demanded the retreat of the U.S. from interests in the middle east and South Korea, threatening nuclear warfare in the case of North Korea[5].

---

[1] National Security Strategy of the United States. December 2017. *The National Security Strategy focuses specifically on the threats posed by China, Russia, Iran, and North Korea where non-state actors such as Al-Qaida are also identified but limited global strategic value is attributed to defense beyond the homeland. Specifically, the call for the United States to "rethink" the incorporation of the major power states in international bodies such as the UN, WTO, and others was viewed by the Trump Administration as a method for isolation of these powers from their base support as compared to previous administration approaches to bring these powers closer to democracy by giving them a voice in international politics.*

[2] The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: September 2018). *The National Cyber Strategy outlined a number of initiatives and based on the pillars of the National Security Strategy. These include combating influence campaigns, mitigating cybercrime, and deterring cyber-attacks against the U.S., both critical infrastructure and persons.*

[3] National Intelligence Council; Global Trends: Paradox of Progress. January 2017. *Near Future: Tensions are Rising (pgs. 29-44).*

[4] *State-level agreements will ebb and flow based on the immediate resource needs of each particular state.*
See Also: Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative", Council on Foreign Affairs, January 28, 2020. (https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative). *China's Belt & Road initiative is likely to undercut trade balances with the U.S.*
See Also: Artyom Lukin*; Opinion: Putin's Silk Road Gamble;* The WorldPost via The Washington Post. February 8, 2018. (https://www.washingtonpost.com/news/theworldpost/wp/2018/02/08/putin-china/) *Russian consolidation of former Eastern Bloc nations providing a gateway to trade imbalances and extreme regional influences.*

[5] National Security Strategy of the United States. December 2017. *See Also:* Patrick McEachern, "What Does North Korea Want." The Foreign Service Journal. October 2019. (https://afsa.org/what-does-north-korea-want)

The new approach called for by leadership demands that a whole-of-government response be utilized to assure our national security and national interests are maintained[6]. Additionally, horizontal and vertical escalation tools, techniques, and procedures are required to assure the U.S. that dominance and supremacy is unmatched. In this report, we consider this approach to be defined as Integrated Deterrence.

To meet the challenge of Integrated Deterrence, we have defined here a methodology to comprehensively assess deterrence tools and the range of strategic threat actions that each tool could credibly deter. The comprehensive nature of the methodology is based on qualitative probabilistic assertions where strategists can use constructivist logic to determine adversarial costs and benefits and apply this logic to determine if deterrence tools will be effective in a systematic approach. Importantly, this framework recognizes that the credibility of a deterrent tool is not only a function of the technical capability of that tool, but on the sociological concept of the principle of proportionality. The latter being the principal driving need to align the proper deterrence tool with a given threatening action. Furthermore, support of deterrence tools conclusions is built upon a detailed assessment of tool requirements and hardware components that are realized to make the tool a credible deterrent.

While we define the framework for a systematic assessment of the U.S. deterrent architecture, such a comprehensive analysis is beyond the scope of this project. However, to demonstrate how such a framework can be utilized in practice, we provide a detailed case study of one deterrent tool, a Secure Nuclear Weapon 2nd Strike, to deter a single adversary action, a massive nuclear first strike upon the U.S. This deterrence tool-to-action pair provides a proportional response to an aggressive action that enables this report to assess what is arguably the most important deterrence capability our nation possesses and focus on specific science and technology aspects of the capability. For this analysis, we define the tool mission requirements based on the capability concept of operations, the mission "kill-chain," and we define the key representative sub-components that must be realized to effectively field the capability. We perform a detailed assessment of the components of the defined Secure 2nd Strike relative to the mission "kill-chain" requirements. This enables focus on science and technology (S&T) aspects in key areas of scientific knowledge, and gaps and limitations therein, to determine likely S&T trends as well as technical S&T solutions that can enhance or degrade the Secure 2nd Strike tool as a credible deterrent in future threat space.

As national threats continue to evolve, so should U.S. tools and the assessments of them. Given the wide variety of threats we face as a nation, this report represents a starting point for an assessment at-large of credible deterrent tools that face the nation. This scope of work can be approached under the guidance of knowledgeable national security strategy subject matter experts and be employed from the greatest of threats to the most benign. As deterrence solutions are realized for the spectrum of threat actions, and each capability is optimized for effectiveness to specific actions, the United States will become better postured to shift focus to deterring actions that impact citizens' daily lives such as cyber and gray-zone conflict scenarios.

---

[6] Michael Clarke. *Back to the Future: Is 'Integrated Deterrence' the New 'Flexible Response?'*. The National Interest; 23 October 2021. (https://nationalinterest.org/feature/back-future-%E2%80%98integrated-deterrence%E2%80%99-new-%E2%80%98flexible-response%E2%80%99-195274)

Throughout this report, we focus significantly on the methodology and science and technology aspects of our analysis capability developed herein with the goal of ensuring this capability can maintain three primary goals:

1) Define the "landscape," or spectrum of actions that would require deterrence;
2) Provide insight for how effective the current nuclear weapon capability is to deter the postulated threat-actions; and
3) Develop an assessment for what science and technology areas provide enhancement of the nuclear weapon deterrent as well as what S&T areas will degrade the nuclear deterrent capability.

We have deliberately chosen to not discuss detailed resolve of conventional warfare and cyber warfare tools within this report due to the subject matter expertise of the authors and the vested interests of Lawrence Livermore National Laboratory. Therefore, while the concepts and methodology apply to these categories of conflict, the majority of the examples and case study within this report focuses specifically on the applicability of nuclear weapon deterrence missions.

The Calculus of Deterrence

Deterrence – broadly defined as the act of instilling doubt or fear to discourage someone from doing something – has been an implicit element of the U.S. national security reaching its height of import during the Cold War. Many scholars have previously discussed methods and models to examine and explain when deterrence will be successful. Within this report we build upon a method that develops a qualitative gauge through an inequality as the measure for successful deterrence that can be applied to deterrence models such as deterrence by punishment, deterrence by denial, and others such as deterrence through encouraging restraint[7], entanglement[8], resilience[9], etc. Given the imprecise definition of most of these concepts and their interrelation, it is not surprising that it can at times be difficult to understand the relative import of one method of deterrence over the other, or even distinguish between some of the methods[10].

To develop the basic terms used within this report, we highlight the underlying intentions of deterrence by punishment and deterrence by denial. Deterrence by punishment not only depends on the threat from the deterrer of imposing a cost on an adversary given an adversary's action, $\mathrm{cost(action)}$, but the probability of imposing that cost conditioned on the adversary's action $p(\mathrm{cost}|\mathrm{action})$[11]. Deterrence by denial, which seeks to deter an adversary by denying their potential benefits of carrying out a hostile action, uses the same type of conventions when defining each term, where $\mathrm{benefit(action)}$ is the value

[7] DoD "Deterrence Operation Joint Operating Concept", Version 2.0, December 2006
[8] Joseph S. Nye Jr, "Deterrence and Dissuasion in Cyberspace," International Security 41, no. 3 (2017): 44-71
[9] Guillaume Lasconjarias, "Deterrence through Resilience - NATO, the Nations and the Challenges of Being Prepared", NATO Eisenhower Paper 7, Research Division - NATO Defense College, Rome May 2017
[10] For example, it is not entirely clear what the distinction between deterrence by denial and resilience are. It seems as though resilience attempts to deny one's adversary their objective of causing long-term harm to you by being resilient to their attack, which would then make it at most a subcategory of deterrence by denial.
[11] A concept central to the strategy of the threat that leaves something to chance (Schelling, 1906 p187; Schelling 1966 p92).

of the benefit the adversary might receive as a result of their action and $p(\text{benefit}|\text{action})$ is the probability of that benefit being realized.

Given the widespread and lasting importance of deterrence it is not surprising that all of the general deterrence concepts necessary to develop a complete and explicit formula exist in one form or another in the vast amount of existing related literature. We do however believe it is necessary to combine them in a complete explicit form that allows us to develop a complete logic for use our systematic deterrence assessments. Several authors have even expressed the deterrence calculus in explicit form, albeit incomplete and typically relegated to the footnotes[12]. In other words, assuming rational actors, we achieve deterrence when our adversary perceives that the probable costs of their action ($p(\text{cost}|\text{action}) \times \text{cost}(\text{action})$) is greater than the probable benefits they might receive as a result of that action ($p(\text{benefit}|\text{action}) \times \text{benefit}(\text{action})$), or more explicitly:

$$\frac{p(\text{cost}|\text{action}) \times \text{cost}(\text{action})}{p(\text{benefit}|\text{action}) \times \text{benefit}(\text{action})} > 1$$

Equation 1

Each of the terms in Equation 1 is a function of the adversary's action. In other words, the cost one threatens to impose depends on the action they are deterring. Thus, an effective deterrence will maximize perceived adversarial costs paid to carry out a given action as well as their perceived probability of having to pay that cost. At the same time an effective deterrence will minimize, or deny, the benefits that adversaries expect to receive from carrying out their action as well as the estimated probability of receiving that benefit.

While Equation 1 is explicit, we do not consider it complete. As Shelling notes, "any coercive threat requires corresponding assurances; the object of a threat is to give someone a choice"[13]. To complete the deterrence calculus formula, we must account for the fact that the rational adversary simultaneously weighs the potential costs and benefits of carrying-out the action with those costs and benefits of <u>not</u> carrying-out the action ($\sim action$). This is equivalent to accounting for the concept of encouraging restraint[14]. In other words, it is possible to encourage adversary restraint by decreasing the probability of a negative cost being imposed on them when they don't engage the hostile action ($p(\text{cost}|\sim\text{action}) \times \text{cost}(\sim\text{action})$), or similarly increasing the probability of reward if they don't engage the hostile action ($p(\text{benefit}|\sim\text{action}) \times \text{benefit}(\sim\text{action})$), in addition to denying benefits and imposing costs. In our explicit form, combining the concept of encouraging restraint with Equation 1,

[12] Perhaps one of the earliest is Bruce Russett's "The Calculus of Deterrence, 1963, The Journal of Conflict Resolution Vol. 7, No.2, pp. 97-109", esp. p. 107 footnote 14. I can only guess that no one has formulated these concepts into a complete and explicit form due to the repellence of mathematical notation in the field. I have experienced few things less constant than this response, and also think back to Schelling's preface to the 1980 edition of "The Strategy of Conflict". Glaser provides an explicit formulation of the calculus of deterrence being successful if "(Probability of U.S. carrying out threat X Costs if threat carried out) > (Probability of accomplishing the action X Benefits of the action)", Charles L. Glaser, "Analyzing Strategic Nuclear Policy", 1990, Princeton University Press, Princeton New Jersey, p. 20. Note that this explicit formulation is also relegated to the footnotes.
[13] Schelling, "Arms and Influence", p74
[14] See for example the DoD "Joint Operating Concept: Deterrence Operations", Dec. 2006

$$\frac{p(\text{cost}|\text{action}) \times \text{cost}(\text{action}) + p(\text{benefit}|{\sim}\text{action}) \times \text{benefit}({\sim}\text{action})}{p(\text{benefit}|\text{action}) \times \text{benefit}(\text{action}) + p(\text{cost}|{\sim}\text{action}) \times \text{cost}({\sim}\text{action})} > 1$$

Equation 2

Fundamentally the terms of Equation 2 are described as the eight levers of deterrence and complete the concept of an explicit form for deterrence. Furthermore, the eight levers of deterrence also provide holistic logic where all terms are required for appropriate assessment of deterrence influence and there can be no additional influence outside of these terms. In light of the explicit form defined here, successful deterrence then implies maximizing the numerator relative to the denominator.

We postulate that a tool is 'good at deterrence' when Equation 2 is qualitatively satisfied[15]. So, what does it means to be good at deterrence? As we argue, this more complete representation significantly influences the conclusions drawn about science and technology implications for deterrence tools. Perhaps the most relevant example of this is, the fact that the cost of inaction ($\text{cost}({\sim}\text{action})$) is an inherently difficult lever to manipulate to change the deterrence calculus. This is primarily because deterrence tools that can impose a cost if the adversary carries-out an action are often capable of punishing the adversary even if they don't carry-out an action (i.e., $\text{cost}(\text{action})$ is highly correlated with $\text{cost}({\sim}\text{action})$) due to the nature that a tool or capability is designed to function irrespective of the adversaries choices to act or not (i.e., 'dual-capable'). Similarly deterrence tools that are capable of denying benefits are also capable of imposing costs (i.e., decreasing $p(\text{benefit}|\text{action}) \times \text{benefit}(\text{action})$ is often correlated with increasing $\text{cost}(\text{action})$ and $\text{cost}({\sim}\text{action})$). This is at the heart of the security dilemma. For example, nuclear weapons work as a deterrent because they can impose an incredibly large cost (i.e., $\text{cost}(\text{action})$ is large). However, assuming a secure nuclear capability, nuclear weapons can impose their cost irrespective of an adversary's action (i.e., $\text{cost}_{NW}(\text{action}) = \text{cost}_{NW}({\sim}\text{action})$). Thus, these terms counterbalance each other in Equation 2. Nuclear weapons work as a deterrent because the probability of launching a nuclear attack on someone if they don't carry-out a hostile action is fortunately very small (i.e., $p(\text{cost}_{NW}|{\sim}\text{action})$ is small). Perhaps in an ideal world there would be such a thing as perfect and purely defensive capabilities and one could decouple the cost of inaction lever ($\text{cost}({\sim}\text{action})$) from the others. Ultimately though the offensive-defensive (i.e., dual-capable) nature of much of a nation's power ensures that the unintentional threatened cost is approximately equal to the intentional threat cost (i.e., $\text{cost}({\sim}\text{action}) \approx \text{cost}(\text{action})$).

Given the coupling of the cost of action and in-action terms, it becomes all the more important to skillfully increase the probability of imposing a cost in response to an adversary's hostile action term ($p(\text{cost}|\text{action})$) and decrease the probability of imposing a cost even if the adversary doesn't carry-out the hostile action term ($p(\text{cost}|{\sim}\text{action})$) term if one wants to favorably manipulate the overall deterrence calculus. Otherwise, there is potential for the terms in the numerator and denominator to balance each other out and there be no net deterrence effect. This is a theme that proves important in the detailed science and technology assessments that follow. However, manipulating these terms in opposite direction is easier said than done[16]. If one must carry out actions that may be perceived as

[15] Much in the same spirit as mathematician Glenn Shafer when he noted that, "Probability is not really about numbers; it is about the structure of reasoning." Note however, that this formalism is extendable to a more complete engineering and intelligence informed quantitative assessment.

[16] Appearing more threatening to increase the adversary's perceived probability that we will follow through on our threat ($p(\text{cost}|\text{action})$) would seem to be positively correlated with an adversary's perceived probability of

threatening to deter a given adversary[17], then it is important that the threat should be perceived as justified to all other observers (or at least the subset of observers whose deterrence calculus you care about). In other words, ensuring that your threats are consistent with relevant laws and norms as well as not making a mistake and imposing a cost when an adversary didn't carry-out the would-be deterred action.[18] Similarly, a clear declarative policy can help provide empirical evidence to decrease the uncertainty associated with the two cost imposition probabilities.

Credibility as a Function of Science & Technology and Proportionality

While we have now defined when deterrence will work (Equation 2), we still need to determine if a deterrent tool will work to deter a given action. In other words, what makes a deterrent tool credible? To answer this, we need to understand what influences the values of the eight levers of deterrence[19]. As we discuss in this section, credibility is determined by two principal variables: the scientific and technical credibility of the tool, and the principle of proportionality. As will be discussed in later sections of this report, technical credibility is assessed through development of key mission requirements and components for realized products that will impose costs. The principle of proportionality qualitatively asserts that for a deterrent tool to be deemed credible that the costs imposed against, or benefits denied by, an action are commensurate to the magnitude of costs received from the aggressor.

Technical Capability

Clearly the technical capability of the tool matters. If the tool is physically incapable of imposing a given cost, then the tool will be ineffective as a legitimate deterrence capability regardless of the action you wish to deter[20]. Additionally, if a tool is technically dual-capable, having both defensive and offensive capability, then this will potentially simultaneously influence several levers of deterrence[21] often in counterproductive ways, as was discussed in the previous section. Through the case study in this report, we develop an argument for when technical credibility is determined viable based on the threat concept

---

imposing a cost on them irrespective of their action (i.e., $p(\text{cost}|{\sim}\text{action})$). Especially after carrying-out a prior threat, and especially if that cost imposition may have been made in error. It is easy to imagine that both the $p(\text{cost}|\text{action})$ term and the $p(\text{cost}|{\sim}\text{action})$ term increased for many countries' perception (Since it is so important a concept it is worth the aside to explicitly state what may be obvious to many. Threats and actions taken to deter one adversary will affect the deterrence calculus of all other observers.) of the U.S. after the 2003 invasion of Iraq and especially after it was revealed that there were no viable weapons of mass destruction (Hoar, Jennifer. "Weapons Found In Iraq Old, Unusable". June 23, 2006. CBS News. Archived from the original on 1 April 2019. Retrieved 02 September 2021.), which was the justification for the invasion.

[17] And it appears that this is sometimes the case, recall the aforementioned discussion about the inefficiency of the pre-2018 U.S. cyber deterrence policy because it lacked the credible threat of cost imposition.

[18] *See Also:* Patrick McEachern, "What Does North Korea Want." The Foreign Service Journal. October 2019. (https://afsa.org/what-does-north-korea-want). *One could argue that this is the reason for failure of U.S. policy to deter North Korean ambitions to achieve nuclear weapon parity in the region. North Korea believes fundamentally that employment of U.S. nuclear weapons in the region are for coercive tactics to effect regime change and therefore, based on the empirical evidence for the U.S. invasion of Iraq in 2003, nuclear weapons are also the only tool at their disposal to deter the United States from imposing a regime change against the Kim Jong Un leadership.*

[19] For example, what increases $p(\text{cost}|\text{action})$, what decreases $p(\text{cost}|{\sim}\text{action})$ and $p(\text{benefit}|\text{action})$? For our study we do not consider the $p(\text{benefit}|{\sim}\text{action}) \times \text{benefit}({\sim}\text{action})$ lever since it is not highly relevant to our LLNL sponsor. As this lever is less influenced by science and technology and more so by economic and diplomatic deterrent tools.

[20] In other words if a tool cannot physically impose cost (x), then $p(\text{cost} = x|\text{action}) = 0$.

[21] $p(\text{cost}|\text{action})$, $p(\text{cost}|{\sim}\text{action})$, and $p(\text{benefit}|\text{action})$ to be specific

of operations and the capability requirements with associated hardware that meets the proposed operational need.

Technical capabilities are necessarily complex due to the inherent need to satisfy political, diplomatic, and physical parameters simultaneously. This complexity provides and introduces mechanisms for failure of the capability and through failure modes that influence both the specific cost imposed or benefit denied, but also the probability that a cost will be imposed, or benefit denied. As we explore further in subsequent sections, technical failure modes for tools may have effects ranging from immediate to incremental based on the severity of the failure mode to the capability.[22] To clarify distinction between actual and perceived changes in the deterrence calculus in this report, we have relied on application of fundamental systems engineering approaches to the complex operations and needs of a deterrence capability.

Within the spectrum of nuclear weapon technical capabilities, the United States has a long and storied history of fielding highly capable and certified nuclear weapons. These weapons are designed and based upon proven nuclear physics that was tested through more than 1000 above-ground and underground nuclear tests until 1992. These tests have proven without a shadow of doubt the ability of nuclear weapons to impose high measures of cost to our adversaries. Since 1992, the United States has relied upon the stockpile stewardship program to ensure that nuclear weapon designs are viable and ready to meet the needs of U.S. national security. Stockpile stewardship is built upon a complex set of activities, performed by Nuclear Weapon Laboratories within the National Nuclear Security Administration within the Department of Energy, including computational testing, modeling, non-nuclear testing, surveillance, and assessment, that culminate with assurance of nuclear weapon reliability, performance, and safety throughout the range of mission requirements. This assurance provides both high confidence and absolute certainty in the nuclear weapon deterrence capability to impose costs to aggressive actions as well as the probability that costs will be imposed as conditioned on the actions of the aggressor.[23]

Principle of Proportionality

The technical capability of the tool, however, is not all that matters. For example, the U.S. has arguably the most capable nuclear weapon deterrent tool of any nation; capable of imposing a cost far exceeding any potential benefit that another nation might receive from any conceivable action. Why then don't U.S. nuclear weapons deter all hostile actions? There is clearly some reason our adversaries think that we will not use our nuclear deterrent in response to all hostile actions, since we have proven our nuclear capability many times over and our adversary can have little doubt that our nuclear weapons will work with high probability. Just as our previous nuclear use, both in wartime and peacetime, has provided our adversaries with significant evidence that our nuclear weapons are technically capable of imposing a large cost with high probability, our non-use of nuclear weapons in response to adversary actions over the past approximately seven-decades, ranging from espionage to deadly attacks on the U.S. homeland,

[22] Specifically, failure mechanisms are the degradation of a capability through loss of subsystem functionality resulting in decreases in $\mathrm{cost(action)}$ and increases in $\mathrm{benefit(action)}$. However, impact to the deterrence calculus may also be realized by decreases in the $p(\mathrm{cost|action})$ and $p(\mathrm{benefit|action})$ terms due to associated confidence factors in the functionality of the subsystems. Conversely, failure modes are the categories of failure by which a capability may become ineffective and in the context of this report, we discuss these modes as changes in anti-access/area denial (A2AD) and missile defense, which more directly influence the perception of terms within the deterrence calculus.

[23] Maximum increase to the $\mathrm{cost(action)}$ and the $p(\mathrm{cost|action})$ terms.

has provided our adversaries with significant evidence that the probability of using nuclear weapons in response to most actions is near zero. This is empirical evidence, but there must be some underlying rationale for why the U.S. has not used nuclear weapons in response to any of these hostile actions, or even threatened their use in most cases. The intuitive answer is that it simply wouldn't be credible to use nuclear weapons in response to a common espionage or cyber-attack. Threatening to respond with a nuclear launch would do more harm to U.S. reputation and moral standing than could possibly be gained from the threat of using them against the postulated action. While this may be true, neither this nor the empirical reason bring us any closer to understanding the underlying rationale for why nuclear weapons are not a credible deterrent against most action, which we must do if we are to confidently answer the question, "What are nuclear weapons good at deterring?". We must also understand this rationale if we wish to understand how best to enhance our nuclear deterrent.

Some might posit that the U.S. fears retaliation; escalation to nuclear use instills fear that adversaries would retaliate with nuclear use. While this logic surely plays a role in some scenarios (e.g., between the U.S. and the Soviet Union during the Cold War, or perhaps between India and Pakistan during the 1999 border war at Kargil[24]), this provides an incomplete answer. In the seventy-six years since the only use of nuclear weapons against a foe, there have been at least nine wars between a nuclear armed state and an unarmed state where nuclear weapons were not used[25]. Some of which were lost by the nuclear armed state. So some might also attribute the lack of nuclear weapon use to the *nuclear taboo*, or the "de facto prohibition against the first use of nuclear weapons."[26] The nuclear taboo is merely the name of a norm. We must understand why this taboo exists if we wish to understand its implications for the enhancement or degradation of our nuclear deterrent, when we might expect the norm to be broken, or its implications to integrated deterrence as a whole.

At the core of the nuclear taboo, is the long-standing moral principle of proportionality[27]. Put generally, the principle of proportionality states that the cost of the retaliatory action should be approximately equal to the cost of the original offending action(s). For a threat to be credible in deterring an action, it is typically assumed that it must abide by the principle of proportionality (i.e., $\text{cost}(\text{threatened action}) \approx \text{cost}(\text{action wishing to deter})$, see Figure 1). The principle of proportionality is the analytical perspective we use achieve our objectives of determining what nuclear weapons are good at deterring, as well as how best to enhance them or supplement them with other integrated deterrence tools. That said, the logic behind this principle must also be understood to use it with

---

[24] S. Paul Kapur, "India and Pakistan's Unstable Peace: Why Nuclear South Asia is not like Cold War Europe", *International Security*, Vol. 30, No. 2 (Fall 2005), pp. 127-152.

[25] Thomas Shelling points out that nuclear weapons were not used in the United Nations' defense of South Korea, the succeeding war with the People's Republic of China, the U.S. war in Vietnam, the 1973 war between Egypt and Israel, the British war with Argentina, nor the Soviet Union against Afghanistan (Schelling, *Arms and Influence*, Preface to the 2008 Edition). We can add to this list the 1991 US-led war against Iraq, the NATO war in Afghanistan from 2001-2021, and the U.S. war against Iraq starting in 2003. Perhaps most interestingly, several of these wars were lost by the nuclear armed state.

[26] Nina Tannenwald, "Stigmatizing the Bomb: The Origins of the Nuclear Taboo," *International Security*, Vol. 29, No. 4 (Spring 2005), pp. 5-49.

[27] While Nina Tannenwald notes this, she also argues that the principle of discrimination is also at the core of the nuclear taboo ("Stigmatizing the Bomb: The Origins of the Nuclear Taboo," *International Security*, Vol. 29, No. 4 (Spring 2005), pp. 5-49.). We will not discuss the principle of discrimination since it is a derivative of the principle of proportionality.

confidence within the construct of the deterrence calculus framework and to understand when conclusions based on this assumed principle may become tenuous or invalid[28]. In other words, while the principle of proportionality is often argued from a moral perspective, it is unsatisfactory, for our purpose of creating a general and systematic tool, to hinge the logic on the ill-defined and culturally dependent concept of morality.

As it turns out, understanding the principle of proportionality flows from the understanding of the principles of deterrence calculus, Equation 2, as discussed previously[29]. Violating the principle of proportionality in a given instance will increase the perception that an actor is a bully for all observers, thereby instilling fear that that actor might impose an unfair cost on them in the future without justification from a specific action[30]. This will negatively affect the observers' calculus towards the offending nations' self-interests[31]. To be specific, violators of the principle must be concerned with potential balancing[32], both externally (e.g., other nation states), as well as internally (e.g., one's own domestic constituents). There have been actions taken by broad swaths of humanity to increase the probability of balancing in response to non-proportional actions by adopting the principle of proportionality as a social principle[33] and codifying it in international law[34] with violations of it constituting a war crime[35]. Thus, the principle of proportionality can be understood purely in terms of the deterrence calculus with the concept of morality only serving as a vehicle to achieve a decision calculus state that is more favorable to the majority of humans. This also enables us to understand when the principle of proportionality is unlikely to have meaningful influence on the deterrence calculus.

---

[28] Or as Thomas Shelling notes in *Arms and Influence*, p148, "Even when this tendency to act in patterns – to respond in the same idiom, to make the punishment fit the crim in character as well as intensity – has been explained it still deserves to be evaluated; the fact that it come naturally does not mean that it necessarily embodies the highest military or diplomatic wisdom." By his evaluation, "bureaucracies have a propensity toward casuistry, legalistic reasoning, and philosophical neatness that makes nation leaders instinctively act in a coherent patter." Again this answer is too far disconnected from the fundamental decision calculus governing the behavior of people, Equation 3, to be satisfactory.

[29] While George Quester suggests one never conducts a cost/benefit analysis in the case of a taboo ("The End of the Nuclear Taboo," On Limited Nuclear War in the 21st Century, Chapter 8, Jeffrey A. Larsen and Kerry M. Kartchner (eds.), Stanford: Stanford University Press, 2014.), we do not believe this is correct. Decision makers still conduct a cost/benefit analysis, it is just that the taboo enables them to do it quickly and without much rigor because the taboo implies that there will be massive social costs to carrying out the action disproportionate to any potential gains.

[30] More technically speaking, increasing $p(\text{cost}|{\sim}\text{action})$ for all observers. These balancing dynamics have recently been observed following the Russian invasion of Ukraine in February 2022.

[31] It is not just outside observers that the offender must be concerned with. They must also worry about the enemy they offended, for it is rarely the case that the enemy will be annihilated. Given that your enemy today might be your ally tomorrow (e.g., the U.S. and Germany, the U.S. and Japan, etc.) there is some incentive to prime your adversary's decision calculus for the period after the war.

[32] Balancing in the sense of upsetting the balance of power by states committing themselves to containing a dangerous opponent. See e.g., John J. Mearsheimer, The tragedy of Great Power Politics, New York, W. W. Norton, 2001, pp. 139, 156-157.

[33] See the "The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law" report from the Internal Expert Meeting, 22-23 June 2016, Quebec, Laurent Gisel (ed.), for an extensive summary of internal law regarding the principle of proportionality.

[34] Article 51(5)(b) of Protocol I of 8 June 1977 additional to the Geneva Conventions (AP I)

[35] Article 8(2)(b)(iv) of the Rome Statute of the International Criminal Court (ICC)

Specifically, when there is no credible threat of balancing, or changing the current balance of power cannot be achieved[36].

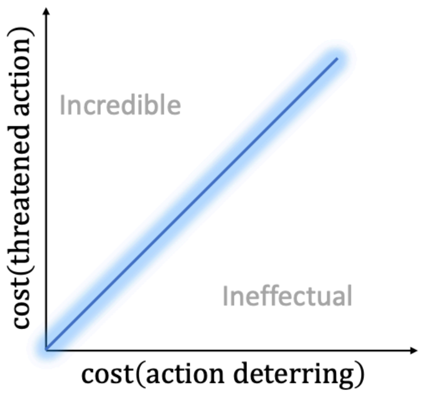

Figure 1: The principle of proportionality states that the cost of the threatened action should be proportional to the cost of the action you are wishing to deter in order to be perceived as credible. The general region signified by the line represents when threats are proportional to actions, however, when threats are not proportional to the action they may be perceived as incredible or ineffectual within the framework of the deterrence calculus.

Therefore, to summarize, we postulate there are two main bases responsible for the principle of proportionality[37]:

1. Concern about increased counter response potential (i.e., retaliation)
2. Balancing concerns, both internally (i.e., domestic) and externally (i.e., international)

When either or both of these bases for proportionality hold, one must factor the principle of proportionality into the assessment of deterrence credibility. When neither of these bases hold, the principle of proportionality can be disregarded and the deterrence calculus will be dominated by the technical capabilities of tools.

The Equivalence Problem

Perhaps the prime difficulty in applying the principle of proportionality, both practically and analytically, is that within the deterrence calculus, actors are often dealing with costs that have no clear equivalence[38]. Thus, it is not easy to determine whether the cost associated with the deterrent threat is

[36] Clearly the principle of proportionality does not influence your decision to stomp the cockroach that happens to wander across the border of your garage (two acts that are hardly proportional). In this simplified example of the cockroach, there is no threat of balancing against the homeowner.

[37] While Nina Tannenwald suggests that there are four pathways by with nuclear taboo developed ("Stigmatizing the Bomb: The Origins of the Nuclear Taboo," International Security, Vol. 29, No. 4, Spring 2005, pp. 5-49.), only two of these are related to the source of the taboo, the other two are a result of the first two and simply act to reinforce the taboo. The two causal pathways are "Societal pressure" and "normative power politics", the first establishing/reinforcing domestic and international balancing concerns, while the later applies to just international balancing concerns. Nina also claims that it is the indiscriminate nature of the weapon that is a source of the taboo, but this is just a derivative of the principle of proportionality and the fact that there is broad agreement that some lives are more valuable than others and to kill an 'innocent' person would be disproportionate to their actions.

[38] We are often comparing apples with oranges. For example, what economic sanctions are equivalent the annexation of Crimea?

approximately equal to the cost that would result from the action one wishes to deter (i.e., $\text{cost(threatened action)} \approx \text{cost(action wishing to deter)}$), because one needs a conversion function $f[\cdot]$ that related the two costs,

$$\text{cost(action A)} = f[\text{cost(action B)}],$$

and this function is ill-defined[39]. Thus, all agents are burdened with the responsibility of estimating the conversion function ($f[\cdot]$) and it is likely that each actor will come up with a different estimate. It is also likely that each actor will attempt to bias this function in their favor through actions, diplomacy, and the establishment of norms (weighing actual costs against their interests as higher than costs against their adversary)[40]. In addition to biasing the conversion function ($f[\cdot]$), our adversaries also take advantage of scenarios where there is considerable uncertainty surrounding the function and attack us with tools where costs are difficult to quantify (e.g., social and cyber actions).

The equivalence problem has, and will continue to have, major implications for deterrence, even more so as the U.S. makes integrated deterrence a larger focus. The more disconnected two actions, both in action type and time, the more difficult it is to estimate and communicate your estimate of what the conversion function ($f[\cdot]$) is to other actors[41]. For example, it is far easier to reach some agreement that the loss of a red armed combatant is a proportional response to the loss of a blue armed combatant than it is to determine what scale of a cyber-attack on blue is proportional to the loss of a red armed combatant. This challenge has led some to the tit-for-tat response philosophy. This is understandable, but not necessary. It is possible to actively define conversion functions ($f[\cdot]$) by clearly connecting responses to hostile actions and diplomatically communicating the function to our adversary, as well as the rest of the world, to mitigate the risk of balancing.

As we will see in the next section, the principle of proportionality coupled with the equivalence problem drives the determination of what actions we assess nuclear weapons are good at deterring.

A Framework for Assessing a Deterrent Capability

Having established the fundamentals of deterrence credibility we now develop a framework for systematically assessing the current U.S. nuclear deterrent capability. We limit our initial assessment to a high-level review of actions where we can posit nuclear weapons may threaten to deter. As we have noted in this report, the complexities of determining technical credibility to perceived costs and perceived benefits are numerous. Therefore, a systematic process for assessing and evaluating the effectiveness of a deterrence capability within the framework of the deterrence calculus must be utilized to provide comparisons for proportionality and equivalence.

To do this, we have applied a modification of the Systems Engineer V-Curve; the Deterrence Calculus Curve (Figure 2), in which we will focus on the concept of operations and resulting high-level

---

[39] For example, there exists no universal measure determining the universal cost of annexing Crimea in terms of economic sanctions.

[40] There are countless examples of this throughout history. The Nazis devaluing Jews as a lesser form of life. Presidential remarks by Harry Truman implying that "the Japanese were subhuman creatures to whom the moral restrain of nations need not apply" (Paul Boyer, *Fallout: A Historian Reflects on America's Half-Century Encounter with Nuclear Weapons*, Columbus, Ohio State University Press, 1998, p. 20).

[41] Schelling, Arms and Influence, p.145

requirements as implemented relative to the basic hardware and implementation of our deterrent. As will be shown later in the detailed assessment, the application of this curve to our problem statement provides unique analysis capabilities and the ability to investigate effectiveness and potential gaps and/or limitations in deterrence tools. The value of using this curve also provides us the opportunity to make certain assumptions within our evaluation assessments where we can focus on the aspects of particular interest to the analysis. For instance, within the context of looking at what nuclear weapons are good at deterring, we rely only on the concept of operations and high-level requirements for analysis under the assumption that nuclear weapons are readily deployed to the field and can impose a technically credible cost under all circumstances. The nuance of statistical technical reliability for nuclear weapon functionality is germane to the magnitude of cost from a nuclear weapon within the deterrence calculus when it is assumed that the weapon will be used as we discussed in the previous sections. We provide a thorough explanation for the rationale of each item within the framework as follows.

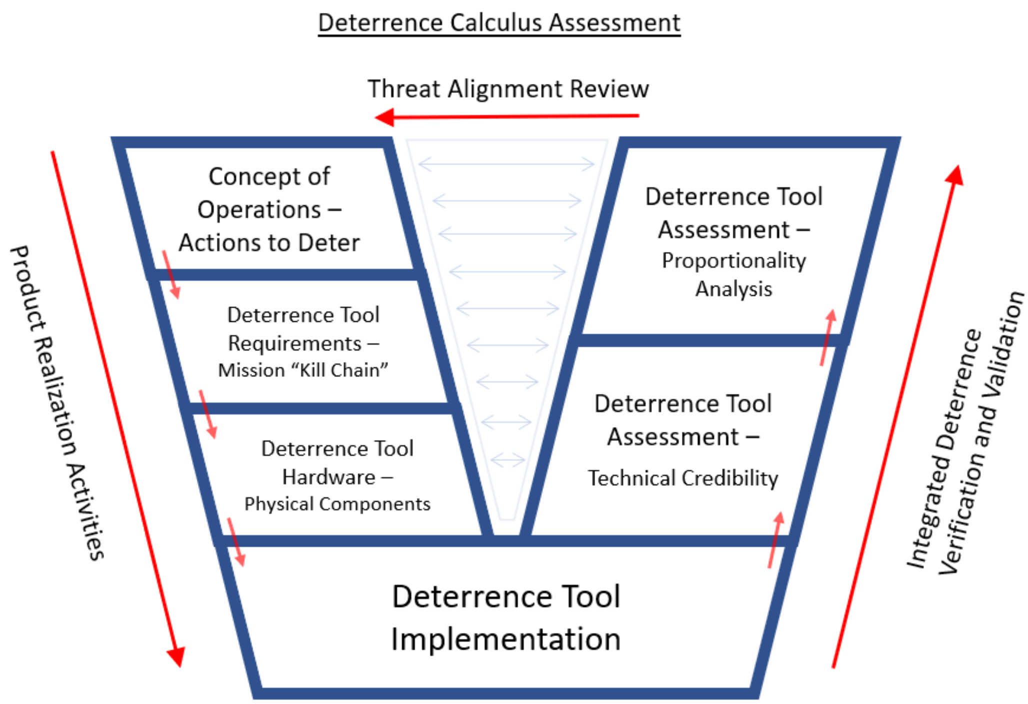

Figure 2: A diagram of the proposed "Deterrence Calculus Curve." The curve starts with high-level development of requirements and hardware based on desired actions to deter and results in assessments of the tools for technical credibility and the principle of proportionality. The process is iterated through deterrence tool reviews to assure the tool is properly aligned to the action and resulting in a favorable deterrence calculus. Modifications to the deterrence tool suite can be appropriately assessed independent of tool capability development actions.

Our methodology is based on a concept of operations that is defined by the adversary actions that we wish to deter. We define these hostile actions as those that impact our concepts of U.S. National Security and negative influence to U.S. National Interests. As will be discussed further in the case study, we have notionally considered the range of hostile actions as those that can influence American society through coordinated cyber campaigns and cyber-attacks against people, conventional conflicts between non-western nation states or against U.S. allies, major cyber or espionage attacks against critical infrastructure, and actions up to and including conventional or nuclear strikes against the United States homeland.

According to game and utility theory, we should prioritize deterring the actions that impose the greatest expected cost[42]. Thus, any rigorous systematic analysis of our overall deterrence capability should start by ordering the actions we wish to deter from least to greatest expected cumulative cost and start the assessment from the costliest actions. Ordering actions, and the progression of our systematic analysis, by expected cumulative cost is conveniently conducive to analyzing the credibility of a given deterrent tool with the principle of proportionality. This is depicted in Figure 3.

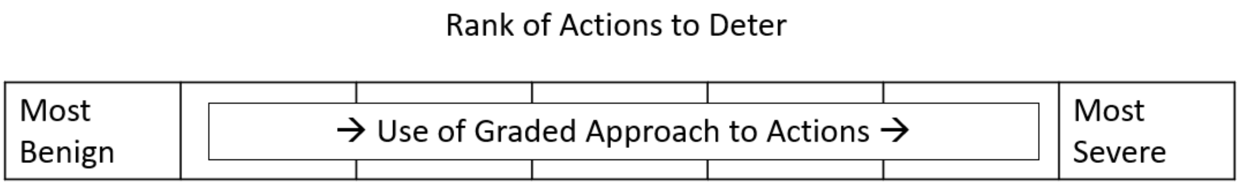

Figure 3: Ranking of Actions by costs incurred. Alignment of actions in normative ordering enables logical assessment consistency and acceptance by critics and allies alike. This alignment is conducive to analyzing the credibility of a given deterrent tool with the principle of proportionality.

As noted previously, deterrence can be affected by several different or even multiple levers, such as through imposition of costs through punishment, denial of benefits, and versions of encouraging restraint. Effective deterrence is based on the United States having credible tools at its disposal that can implement and manipulate these levers as desired against the specific threats. Therefore, having multiple tools to credibly deter the range of actions ranked within this methodology is desirable.

For an illustrated example, we employ a punishment-based deterrence scheme with the cost imposed by our response on the abscissa and probability of imposing a specific level of cost on the ordinate axis as shown in Figure 4. Since an effective deterrence against multiple threats and hostile actions is therefore likely to utilize a variety of tools, some with overlapping capabilities, we have plotted notional tools against a range of actions with increasingly significant costs. However, because the notional spectrum of tools can impose a proportional cost to the action, the tool would be considered credible for this illustrated example. We then plot the effective probability that the tool would impose the desired costs to an action, some with varying success, to show what a notional deterrence scheme for national security would potentially appear as within adversarial deterrence calculus assessments.

---

[42] By expected cost we mean the expectation of the p(cost|action) x cost(action). See John von Neumann & Oskar Morgenstern, *Theory of Games and Economic Behavior*, Princeton, Princeton University Press, 1953 for a game theory proof that maximizing the expected returns is optimal. Or Judea Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, San Francisco, Morgan Kaufmann Publishers, 1988, 2nd ed., pp. 294-299, for related utility theory arguments. Even though people, even rational ones, often make choices which do not maximize the expected return, see e.g., *Choices, Vlaues, and Frames*, eds. Daniel Kahneman & Amos Tversky, New York, Cambridge University Press, 2000 pp. 1-43.

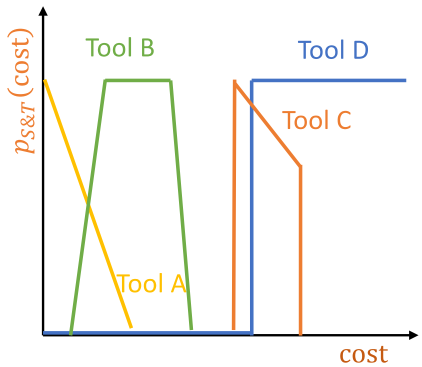

Figure 4: For each blue deterrence tool {A, B, C, D, etc.} the adversary will estimate the probability ($p_{S\&T}(cost)$) that that tool will be technically capable to impose a cost.

As with the approach to organization of the actions one would wish to deter, being from lowest to highest in terms of cost; we use the same approach to organize the potential deterrence tool capabilities. The logical organization from lowest imposed cost against an action to highest imposed cost against an action is illustrated in Figure 5.

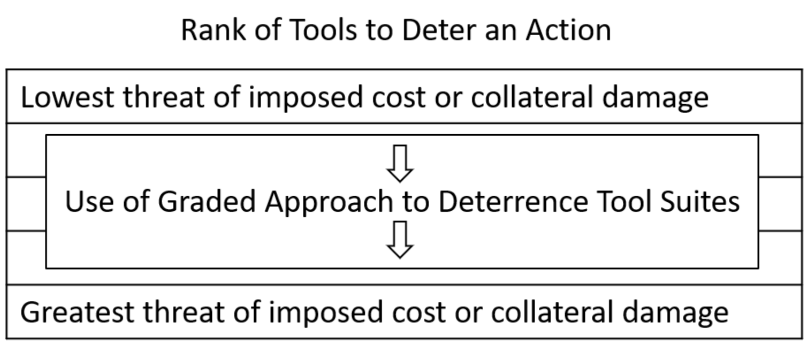

Figure 5: Ranking of Tools to deter an adversarial action. Alignment of tools in normative ordering enables logical assessment consistency and acceptance by critics and allies alike. This alignment is conducive to analyzing the credibility of a given deterrent tool with the principle of proportionality.

The complete concept of operations is then transposed to a matrix where we can develop a matrix for each tool against the specific adversarial threat in discrete forms. To be explicit in terms of the deterrence calculus for notional red (adversary) versus blue (self), for each action i, blue should then consider how the adversary perceives the cost that might be imposed by each of blue's tools j ($j =$ {A, B, C, D}) in the conceptual assessment matrix of Figure 6). In other words, how will red estimate, or perceive, the probabilities for each cost or benefit of action or inaction in the deterrence calculus [43] given blue's tool j; in particular, the tool's technical ability to respond to red's action i as well as the proportionality of the cost imposed by that tool. This ability to transpose the concept of operations into the resulting matrix of tools-to-actions represents the goal of the deterrence assessment methodology and is used in this report as our ultimate assessment for how to correlate the deterrence calculus to the technical credibility and the principle of proportionality in a single snapshot of time. If the resulting ratio

[43] Technically speaking, $p(\text{cost}_j|\text{action}_i)$, $p(\text{benefit}_j|\text{action}_i)$, $p(\text{benefit}_j|{\sim}\text{action}_i)$, and $p(\text{cost}_j|{\sim}\text{action}_i)$, given blue's tool j.

of the decision calculus is greater than 1 then blue's tool is deemed to be a credible deterrent of red's action (e.g., color coded green in Figure 6). If it is less than 1 then the tool is an incredible deterrent and if it is approximately 1 then it is a questionable deterrent (e.g., colored red or yellow in Figure 6 respectively).

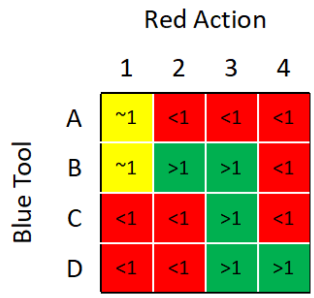

Figure 6: Conceptual 'Red Action' – 'Blue Deterrence Tool' assessment matrix.

Providing critical details of the deterrence calculus assessment matrix is the basis for ensuring that the tool-to-action alignment is sufficient for deterrence. If all of blue's tools are deemed incredible for a given action then red may have high motivation to carry out that action, or if at best any of blue's tools is a questionable deterrent for a given action then it is questionable whether red will carry out that action (e.g., in Figure 6 it is questionable whether red will carry out action 1 because at best blue tools A and B provide questionable deterrent capability). For blue to deter red's action most successfully, it must have at least one tool to provide a credible deterrent capability (e.g., blue tool B will successfully deter red action 2 in Figure 6). That said, some tools may provide better general deterrent capabilities than others (e.g., blue tool B in Figure 6).

In a complete systematic deterrence assessment approach, the above process is repeated for as many red actions as blue wishes to deter. The end product will be a full $i \times j$ matrix of 'red actions'-'blue tool' (see e.g., Figure 6) and the associated deterrence assessment of tool j deterring action i. Since the calculus is a dynamic and qualitative process dependent on the actions of each adversary, as well as the evolving environment in general, this process must be continually updated.

Clearly such a complete systematic deterrence assessment can quickly become intractable since the space of red actions and blue tools is technically unlimited and it is technically possible to continually increase the fidelity of any one assessment. So, some simplifications must be implemented if the general approach is to be made practical.

It may be possible to truncate the analysis by limiting consideration to the actions that have a high cost, including cumulative costs, imposed on blue[44]. It might also be possible to truncate the analysis by considering the tools that blue is likely to use in response to, or threaten against, a given red action. Finally, assuming the principle of proportionality, it might be possible to truncate the analysis to only consider tools that impose a cost proportional to the cost of a given adversary action and proportional deterrence by denial tools. However, we advise caution when considering overt truncation of deterrence tools in diplomatic signaling phases of discussion because the adversary may not know which

[44] It is important to consider cumulative cost since it is possible to have small cost actions that are repeated many times to great cumulative impact. If such an analysis considers just high cost actions it opens the door for the adversary to pursue low cost actions that they can repeat many times (e.g., many of the common cyber attacks).

tools you have or which tools you are likely to use. We do have higher confidence in developing assessments based on the adversary's perception and to drive any assessment truncation before completing the action-tool assessment matrix[45]. There are other potential economies of analysis truncation that should be investigated further, however, we leave those investigations as beyond the scope of this report.[46]

It is vitally important to our methodology to also assure that deterrence tools are not just identified but also implement a technically credible physical solution to meet the tool requirements that can be tested and validated for cost imposition. The holistic scope of this methodology provides a better understanding of effectiveness of a deterrent capability and if it is likely to be successful against the particular action or a range of threats.

Tool Requirements and Assessment Methods

The assessment for each tool to a particular action is broken down to a set of requirements that are necessary and enable the tool to impart the desired cost, or deny benefit, of an action. This mission "kill-chain" is unique for each tool-to-action combination because not all effective costs imposed, or benefits denied, are the same (by design) but represents different phases of the concept of operations or different phases of tool functionality. However, a general flow for requirements will be similar among tools, including fielding hardware, gaining proximity or functional awareness of the target, and imposing the desired costs or denying the intended benefit. For example, within the case study presented in this report, we provide high-level requirements that represent the nuclear weapon "kill-chain" in terms of fielding weapons and delivery vehicles, surviving an adversarial nuclear first strike, and finally imposing cost through the retaliatory second strike.

Mission requirements are supported by physical products and components that are realized through fabrication and assembly and implement the capability as an instrument that can be applied in response to aggressor action. Each of these components is thereby assessed against each of the phase requirements in the mission kill-chain for reliability and performance characteristics that support the probability of the deterrence capability to affect the deterrence calculus. The identification of each physical component to the assessment matrix here allows us to determine gaps, and limitations, of the components in relation to the mission phases and also enables a logical organization of components and hardware that are necessary to validate the tool as a successful deterrent capability.

When considering the focused assessment of each component to the kill-chain requirements, our methodology highlights S&T and trending models that can be used to predict and develop needs and schedules that facilitate blue advantage. The current status of each component in relation to the kill-chain is assessed using informed judgement of the existing snapshot in time. The future minimum status is assessed using pessimistically informed judgement under the consideration that adversarial red players will advance their interests to disrupt the deterrence tool and specifically the mission kill-chain at rates asymmetric to blue players creating or maintaining mission kill-chain and hardware advantages. The future maximum status is assessed using optimistically informed judgement under the consideration

[45] As with all deterrence considerations, estimating what your adversary perceives is often the greatest challenge.
[46] For example, you might be able to estimate the marginal $p(\text{cost}_j|\sim\text{action}_i)$, for all actions i by estimating $p(cost|no\ action\ at\ all)$. Or at least the latter may be a limiting bound on the potential cost. Similarly, with $p(benefit|no\ action\ at\ all)$.

that blue will advance our technological capability in the mission kill-chain at a rate more quickly or innovative than adversarial red players and thereby maintain or enhance the effective deterrent tool.

Within both future minimum and future maximum detailed assessments, the impact of S&T to manipulate multiple levers of deterrence concurrently and simultaneously should be considered and assessed. The culmination of current and future minimum and maximum assessments can be trended qualitatively to determine the vector of the rate of change away from the current state. Finally, the impact of the current assessment combined with trends is assessed relative to crisis stability and dual-capable influence within the deterrence calculus.

Case Study for Assessing the Effectiveness of Nuclear Weapons to Deter

As has been previously discussed, a comprehensive analysis of the full suite of U.S. deterrent capabilities is far beyond the scope of the current project. Therefore, we have chosen to provide an example where we analyze the effectiveness of the U.S. nuclear weapon deterrent tools across a range of possible actions the U.S. might wish to deter. We chose to focus on these tools because it is arguably the most important deterrent capability within the U.S. toolset.

Following the logic and framework previously outlined above, we first determine the coarse list of adversary actions the U.S. might wish to deter. Then we attempt to determine which of those actions nuclear weapons are good at deterring by broadly assessing their technical capability[47], and apply consideration of the principle of proportionality affecting the deterrence calculus. This high-level assessment of nuclear weapon tools culminates in a general outline depicting when nuclear weapon responses provide incredible, questionable, and credible deterrence.

Because of the high confidence in the current technical capability of our nuclear weapon arsenal, the initial analysis of "what are nuclear weapons good at deterring?" is limited by the principle of proportionality. We reach the conclusion that the action we need to deter most is a massive nuclear first strike attack on the U.S. homeland, and that the principle of proportionality states this is an action the U.S. nuclear arsenal is credible in deterring, we conduct a more detailed science and technology focused assessment of how this deterrent might be enhanced or degraded by S&T development efforts and trends within S&T categories in the subsequent sections of this report.

In consideration of nuclear weapon deterrence effectiveness, we also consider the end-state objectives of a capability with respect to conflict resolution:

- Resiliency (survival) against a massive first strike;
- De-escalate gracefully upon initial first and second strikes; and
- Recover rapidly after conflict has concluded.

Notional Actions with Implications to United States National Security

For this report, we have considered a broad range of actions with which we illustrate qualitatively at the highest level when we believe nuclear weapon tools are credible and effective to deter. The range of actions is based on the current security environment and current events as well as anticipated tactical

[47] A detailed technical assessment will be conducted in the following section in the context of deterring the action of a massive nuclear first strike against to the U.S.

and strategic actions within the national security envelope. Our list of notional actions is shown in Figure 7.

Cyber Attack: Persons and Non-critical Infrastructure	**…**	**Conventional War with Non-Ally**	**Conventional War on Ally or NATO**	**Tactical Theater Nuclear War**	**…**	**Cyber Attack: Crippling U.S. Critical Infrastructure**	**Limited Nuclear Strike on the U.S. Homeland**	**Massive Nuclear First Strike on the U.S. Homeland**

Figure 7: Notional Actions postulated for the Deterrence Capability Assessment Case Study.

The lowest and most benign (or common) example of an action chosen for this case study is the example of a cyber-attack against persons and non-critical infrastructure. Examples of these types of attacks are ubiquitous, such as identity theft and the attacks against the Office of Personnel Management (2015)[48], Sony (2014)[49], and more recently the ransomware attacks against the JBS Meat Company (2021)[50]. Given the frequency of these hostile actions against the U.S. there is strong empirical evidence that the U.S. nuclear deterrent does not deter these types of actions. We can understand this in the context of the principle of proportionality with these attacks being grossly un-proportional to nuclear weapon use[51]. As discussed in the previous section we use the principle of proportionality to truncate our analysis of similar low-cost actions and limit our qualitative assessment to more costly potential adversary actions.

In study of our global commitments and influence, we use conventional conflict examples with non-ally nations and allies, including NATO allies, to represent our commitment to extended deterrence mission as outlined by our negotiated accords. Similarly, we use tactical theater nuclear war to represent an escalation of regional conflict, particularly in regions with strong U.S. alliances such as the Baltics or vested economic interests such as Taiwan. While NATO and other partners may demand retaliation through nuclear use, the ultimate decision to use nuclear weapons will reside with what is in America's greatest interests and our commitment to America's allies.

The remaining three scenarios develop conditions where there is a significant and critical threat to the U.S. homeland and a direct correlation to U.S. National Security. These three scenarios are 1) a massive cyber-attack on critical infrastructure as defined through the Department of Homeland Security, Cyber and Infrastructure Security Agency; 2) a limited nuclear strike on U.S. homeland and directly governed territories; and 3) a massive nuclear first strike against the U.S. homeland.

Nuclear Weapon Tools to Deter Actions against the United States

For this case study, we have defined three nuclear deterrence tools that could be authorized by the Commander-in-Chief as a response to the case study actions and are representative of nuclear mission space of interest in this report. We have deliberately chosen to not discuss conventional warfare and

---

48 https://www.opm.gov/cybersecurity/

49 https://resources.infosecinstitute.com/topic/cyber-attack-sony-pictures-much-data-breach/

50 https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs

51 Something the U.S. deterrent is struggling with currently are the many small cost adversary actions that have a cumulative strategic effect (i.e., salami tactics). It appears we have a difficult time perceiving the cumulative cost of many small cost actions.

cyber warfare tools within this report due to the subject matter expertise of the authors and the vested interests of Lawrence Livermore National Laboratory. Our deterrence tools subject to this present analysis are shown in Figure 8.

Low Yield Nuclear Options	Limited Nuclear Options	Massive Nuclear 2nd Strike

Figure 8: Nuclear Weapon Tool Capabilities as established for use in response to adversarial actions. These tools are selected as representative of the Flexible Response strategy employed by many administrations since the 1960s during the Cold War.

Low Yield Nuclear Options represents a tool where the President can tactically respond against a threat with minimized collateral nuclear damage. Yield ranges for these types of weapons ranges from tons to approximately low-tens of kilotons (kt). This report does not correlate any specific weapon systems to yields. Furthermore, this report does not correlate any specific delivery platform to low yield options. This tool does not impede rapid recovery during de-escalation phases of conflict.

Limited Nuclear Options represents a tool where the President can respond with any available nuclear armament to a specific target or set of specific targets with minimal collateral damage to national infrastructure of the aggressor. The intention for this tool is to respond tactically or strategically, without escalation to massive nuclear retaliation, as a demonstrative response to a singular nuclear excursion in areas not vital to geopolitical consequences, most likely to counterforce targets. This tool enables diplomatic strategies to de-escalate gracefully.

The Massive Nuclear 2nd Strike, described herein as the Secure 2nd Strike, is a full nuclear response using all available nuclear forces to annihilate an adversarial target including counterforce and countervalue target sets. This tool, as implied, is designated for response actions and does not imply coercion to achieving threats or dissuading adversarial action.

Assessment of Nuclear Response Deterrence Tools

With the set of tools and the identified actions to deter, the assessment space is well defined to determine if, and when, these tools will be effective. We have qualitatively assessed each of these tools to the actions and have relied strongly on our expert judgement and background in national security policy and stockpile stewardship to present this work here.

From a purely technical capability there are no known tools that can credibly impose such a large cost on an adversary as nuclear weapons. Many nations' nuclear weapons have been proven through tests to be highly capable, so at least for the major powers, there is little doubt that their adversaries assign high technical probability of the nuclear weapons being capable of imposing huge costs. Therefore, as we have stated previously within this report, the usefulness of nuclear weapons as a deterrent is not limited by their technical capability. Thus, nuclear weapon use must be limited by the principle of proportionality[52].

One of the greatest challenges to the general applicability of the nuclear deterrent is that nuclear weapons have a highly inflated perceived cost according to the general public, (see Figure 9). As Nina

[52] Ironically, the DOE/NNSA laboratories have done such a good job with the technical credibility of nuclear weapons that they should focus on other aspects if they want to significantly enhance the U.S. integrated deterrent. As we discuss in the next section though, the technical credibility of the nuclear deterrent is not guaranteed in the future so it still must be tended to.

Tannenwald documents[53], this inflated perception was not always the case. In 1945 the cost imposed by the nuclear weapon attacks against Nagasaki and Hiroshima were largely seen as a continuation of the previous firebombing of Tokyo and bombing campaigns against Hamburg and Dresden, all resulting in approximately the same number of deaths[54]. Beginning in the 1950s, nuclear weapons began to be perceived as very different and their perceived cost began to significantly inflate. The end result being that even though nuclear weapons can impose low costs, these costs would be perceived as much larger than they actually are. Both the public and leaders would worry about balancing against them which is the primary driver behind the principle of proportionality as noted previously. The only conceivable way a low-cost imposition nuclear weapon can credibly deter a low-cost adversarial action is if the adversarial action is subject to a similar inflated perceived costs (e.g., a low-yield or limited nuclear attack).

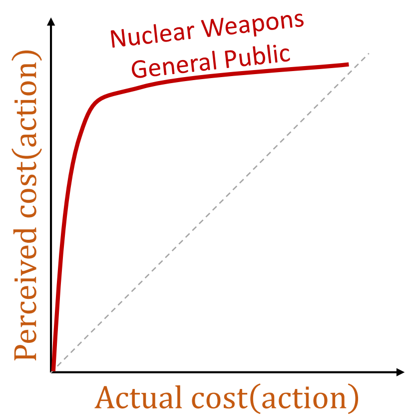

Figure 9: The reason nuclear weapons are not good at deterring a wider range of actions is that they have an inflated perceived cost by the general public, which places them in the incredible region of the Principle of Proportionality space (see Figure 1). This is what underlies the nuclear taboo. Note that other tools (e.g., cyber-tools) can have very different shapes in the perceived versus actual cost space. This is one of the reasons why we see much more prevalent use of cyber-tools. They can impose a significant cost and harder to deter according to the principle of proportionality.

Nuclear weapons also cover a very wide range of cost imposition. In addition to having a large technical probability of imposing a cost at the highest end of the cost spectrum they are capable of imposing costs at the lower end of the cost spectrum. For example, low-yield nuclear weapons can be used to create tactical advantage within the battlefield and mitigate recovery timescales associated with nuclear war. The cost imposition spectrum can further be extended in a continuous fashion to the lower end by detonating the weapons from larger and larger standoff distances[55]. So, it would seem on its face that the principle of proportionality would imply that nuclear weapons could potentially deter low-cost actions[56]. However, this confuses actual cost with perceived cost, and since deterrence calculus is first

---

[53] Nina Tannenwald, "Stigmatizing the Bomb: The Origins of the Nuclear Taboo," International Security, Vol. 29, No. 4, Spring 2005, pp. 5-49.

[54] Barton J. Berstein, "The Atomic Bombings Reconsidered," Foreigh Affairs, Vol. 74, No. 1, January/February 1995, pp. 135-152.

[55] For example, most of the nuclear test during the Cold War were uses of nuclear weapons at the very low end of the cost spectrum. This includes exo-atmospheric studies of Electromagnetic effects (EMP), for example.

[56] Granted, at the very low end the nuclear weapon's cost spectrum, discretization between almost no cost (e.g., from an underground nuclear weapons test) and some appreciable cost (e.g., an EMP or use of low-yield nuclear

and foremost a exercise of cognitive perceptions, it is the perceived cost[57] that clearly matters in this case.

Similar to the importance of perceived cost when determining the credibility of a deterrence tool, our adversary's deterrence calculus will be a function of their estimate of how we will perceive the cost of their action. For this they will use information such as our past actions and stated vital interests (although perhaps to a lesser degree since many political exaggerations are well documented) to estimate how costly we will estimate their action, and should they carry out their action, what tool we will deem proportional to respond with.

For the reasons above, our analysis that produced the conclusions in Table 1 is largely centered on the perceived cost of various actions as well as our assessment of how the adversary might perceive the value the U.S. places on the targets the considered adversary actions.

	Cyber Attack: Persons and Non-critical Infrastructure	…	Conventional War with Non-Ally	Conventional War on Ally or NATO	Tactical Theater Nuclear War	…	Cyber Attack: Crippling U.S. Critical Infrastructure	Limited Nuclear Strike on the U.S. Homeland	Massive Nuclear First Strike on the U.S. Homeland
Low Yield Nuclear Options	Incredible		Incredible	Questionable	Credible		Incredible	Incredible	Incredible
Limited Nuclear Options	Incredible		Incredible	Questionable	Questionable		Questionable	Credible	Questionable
Massive Nuclear 2nd - Strike	Incredible		Incredible	Incredible	Incredible		Incredible	Questionable	Credible

Table 1: While our nuclear arsenal is technically capable of imposing costs across a wide spectrum with high confidence, its deterrent credibility is limited by the principle of proportionality coupled with an inflated perceived cost function. The columns provide a sample from the spectrum of adversary actions the U.S. might wish to deter, order in ascending cost imposed on the U.S. The rows provide a coarse sample of the U.S. nuclear deterrent tools. The colored cells provide our assessment of whether the given tool would be a credible deterrent of the given action (i.e., if the deterrence inequality of Equation 2 is satisfied then the deterrent tool is deemed credible, etc.).

The Principle of Proportionality clearly applies to the use of nuclear weapons in response to cyber-attacks against persons and non-critical infrastructure. Nuclear weapons are a weapon of mass destruction, capable of killing thousands of people through a single use. Cyber-attacks in this small magnitude of damage are rarely capable of inflicting death. Therefore, the use of nuclear weapons to deter these types of cyber-attacks would more likely degrade America's moral standing and create a crisis of confidence in America's rational leadership throughout the world. Thus, we judge the deterrence capability of nuclear weapons in response to threats of cyber-attacks against persons and non-critical infrastructure to be incredible.[58]

---

weapons against troops) results in a relatively large gap. For example, it is difficult to kill just a single individual with even a low-yield nuclear weapon. Thus, there are many adversary actions in the cost gap where the principle of proportionality would clearly state that nuclear weapons are not good at deterring those actions.

[57] As perceived by the deterrer, the deterred, and the outside observers.

[58] The White House, *National Cyber Strategy of the United States of America* (Washington,

When considering conventional wars with non-ally states, our national interests do not extend to the protection of sovereignty of nations outside of the resolution for peace from the international community or a coalition of U.S. partners. In previous examples of these types of conflicts, the U.S. has typically sought to work through international governance such as the United Nations in an attempt to resolve the conflict[59]. Therefore, we judge the deterrence capability of nuclear weapons in response to this threat as incredible because the protection of U.S. national interests or sovereignty of U.S. national security is not affected.

Conversely, under consideration of a conventional war involving an ally or NATO state, our national interests do align with protecting the sovereignty of our ally[60]. We judge that it might necessarily be within the U.S. national interest to employ tactical nuclear forces through either low yield nuclear options or limited nuclear options and maintain the balance of forces and status quo whereby nuclear warfare should not be dismissed as a potential deterrence tool. However, within the context of the deterrence calculus, threatening actors may be strained believe the U.S. would use nuclear weapons first because of the nuclear taboo, which limits the effectiveness of the deterrent tools to questionable.[61] With respect to the remaining nuclear deterrence option, we judge the launch of a massive nuclear strike in retaliation for conventional warfare employed against the ally as an unrealistic response and annihilation of the aggressing nation as not proportional, therefore deeming this tool to be incredible to deter this action.

If either conventional war scenario escalates to use of nuclear weapons or a tactical theater nuclear war, such as has been theorized for conflicts in the region of Taiwan and the Baltics, the use of nuclear weapons is certainly credible. We judge the case for low yield nuclear options to be the most credible due to the minimal collateral damage and tactical nature of the weapons. However, employment of limited nuclear options against counterforce targets including certain military targets not readily within the fighting zone should not be overlooked but is deemed questionable based on our judgement that graceful de-escalation would be the desired strategic motive.[62] The use of the entire nuclear force in a massive retaliatory strike is judged to be incredible, however, due to the implicit assumption that an engagement in this scenario is an engagement with a nuclear-armed adversary. Escalation from tactical to strategic nuclear warfare in this case would likely be met with strategic response from the adversary.

D.C.: September 2018). *The National Cyber Strategy outlined a number of initiatives and based on the pillars of the National Security Strategy. These include combating influence campaigns, mitigating cybercrime, and deterring cyber-attacks against the U.S., both critical infrastructure and persons.*

[59] Many examples in this context exist, including the coalition of U.S. Partners and allies that supported the Operation Desert Storm in Kuwait/Iraq (1991), the Kosovo War (1998), the actions for the Global War on Terror fought within Afghanistan (2001-2021) and the many proxy-wars conducted in the last few decades (Syria, Lybia, Columbia, Yemen, etc.).

[60] This umbrella is reference to those that we have offered extended deterrence to; NATO, Japan, Australia, etc.

[61] Matthew Furhmann and Todd S. Sechser, "Signaling Alliance Commitments: Hand-Tying and Sunk Costs in Extended Nuclear Deterrence," *American Journal of Political Science*, Vol. 58, No. 4 (October 2014), pp. 919-935.

[62] These conflict zones have been discussed numerous times by many different authors. See for example, Rand Corp., RR2781 and Defense Priorities, "Why a Taiwan Conflict Could Go Nuclear", in which many scholars believe that any nuclear options would escalate rapidly to nuclear conflict. Therefore, the point we assert here is the goal of limited nuclear options would be to find a method to de-escalate gracefully as one of the options for conflict resolution.

Within Homefront conflict and direct threats to U.S. national sovereignty, it is conceivable that a massive cyber-attack against critical U.S. infrastructure would impose a cost that warrants escalation and retaliation against the aggressor. In this case, if the attack detrimentally affected infrastructure related to nuclear command and control or our national defense capabilities, we judge that escalation through conventional to nuclear warfare may result. As a matter of clear signaling to aggressors that attacks on the homeland of any kind will not be tolerated, we assess that if escalation to this level occurs, the most likely response will be a limited nuclear strike option as compared to low-yield retaliation or massive retaliation strikes. However, within the deterrence calculus, we assess that the limited nuclear option to deter is questionable because of the equivalence problem as described earlier. The incredibility of the low-yield and massive retaliation options for response is due largely to the principle of proportionality, whereby a low-yield nuclear strike would not convey the extent of our national resolve to protect our national interests and a massive retaliatory strike would impose annihilation costs against harms that will be quickly recovered from.

The deliberate action of a limited nuclear strike against the U.S. homeland or territories would most likely be encountered by adversaries seeking to exclude or deny U.S. national interests in a specific protected territory or possibly as a direct attack for retaliation against international pressures led by the U.S. When faced with this magnitude of action, the U.S. would certainly respond in-kind given our technical capabilities and the principle of proportionality enable a like-for-like response making the limited nuclear option tool a credible deterrent. We also judge the use of a massive retaliatory strike as questionable within the deterrence calculus in order to signal to adversarial networks that the U.S. will intend to quickly eliminate threats and manage or rebuff coordinated attacks against our interests. Similar to the rationale for why low-yield nuclear strikes would be ineffective for deterring massive cyber-attacks against critical infrastructure due to the weak nature of the response, we judge this response to be incredible for this scenario as well.

The most significant of all threats to the U.S. would be a massive nuclear first strike against the U.S. homeland. This type of threat is postulated based on significant adversarial aggression to usurp U.S. global super-power status or to exclude U.S. or western-nation influences from international discussions. The U.S. nuclear arsenal is intentionally designed, based on Cold War experience and motivations, to respond in-kind to this type of attack. We also judge that a limited nuclear retaliation strike may be an option considered as well under certain conditions such as failure of the first strike warheads to reach or impact the designated U.S. target-set. We judge that a low-yield nuclear response would not demonstrate the extent of our national resolve to defend U.S. values, morals, or interests. Because the U.S. capability to field a Secure 2nd Strike response to a massive nuclear first strike is key to U.S. deterrence, we will subsequently provide our detailed assessment, highlighting Science and Technology implications that affect our Secure 2nd Strike capability, as further example of the systematic integrated deterrence analysis presented in this report.

Summary of the Broad U.S. Nuclear Weapon Deterrent Tools Assessment

We have judged the use of nuclear weapons to deter against a first strike to the homeland and that these weapons are expected to deter against nuclear and significant conventional strikes to US allies. The possession of a secure nuclear stockpile provides a strong nuclear deterrent. This deterrent influences the adversary's decision calculus, informing the assumed costs that would be incurred during a second strike, in turn preventing (i.e., deterring) a first strike to the homeland. The knowledge that a secure second strike would inflict more costs than an adversary could gain in benefit, ensures that a reasonable actor would decide not to pursue or coerce through a first nuclear strike. The 2018 Nuclear Posture Review (NPR) indicates (with some level of ambiguity) that the United States would consider, "… the employment of nuclear weapons in extreme circumstances to defend the vital interests of the United States, its allies, and partners. Extreme circumstances could include significant non-nuclear strategic attacks. Significant non-nuclear strategic attacks include, but are not limited to, attacks on the U.S., allied, or partner civilian population or infrastructure, and attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities."[63] These assumptions held true for the entirety of the cold war. As will be discussed next, with the development of new technology, it is clear that an integrated approach to deterrence needs to be taken, in order for nuclear weapons to remain a credible deterrent. We further examine detailed science and technology lines of effort and S&T capabilities of the Secure 2nd Strike capability to explore how S&T can play a fundamental role within integrated deterrence concepts.

How Science and Technology can Enhance and Disrupt our Secure 2nd Strike Deterrent Capability

While we note above that the current credibility of the U.S. nuclear deterrent is driven by the principle of proportionality due to the accepted high technical capability of our nuclear deterrent, new and emerging technologies are shifting trends under the foundation of U.S. technical capabilities. Thus, it is important to not only assess the current technical credibility of the nuclear deterrent but to forecast how science and technology might enhance or disrupt the U.S. nuclear weapon deterrent. This is accomplished through further detailed study using the methodology defined herein for high-level credibility assessments of the mission "kill-chain" requirements and hardware/sub-components supporting the Secure 2nd Strike capability. To manage expectations within the scope of the project while still demonstrating a complete and informed, yet high-level, science and technology assessment as outlined in the framework discussions, we have focused on this single 'blue tool' versus 'red action' element of the overall assessment matrix. In particular, how might science and technology enhance or degrade our Secure 2nd Strike tools' ability to deter a massive first strike on the U.S. homeland.

The technical credibility of the nuclear stockpile is driven by the science and technology that supports the capability. Within the deterrence calculus, this is implicitly considered when using the tool to deter an action. When assessed in detail through mission "kill-chains" and hardware sub-categories, the demonstrated tool could be used to predict the probability distribution of the outcome. Therefore, we continue our case study with a detailed assessment of the kill-chain requirements and tool designs, including cursory verification and validation of the tool as a system of components using our previously defined methodology as shown in Figure 2.

Within this assessment, we acknowledge that subcomponent hardware identification flows from the logic supporting the imposition of costs upon a target while trying to minimize unintentional costs. This logic begins with the identification of a massive first strike threat originating from the adversary and

[63] 2018 NPR, written during the Trump administration, indicates that the United States can employ the use of the nuclear arsenal if any nuclear escalation is pursued. This stance negates the "No first strike" approach and allows for the U.S. to engage in use of nuclear weapons if the attacks are significant. The level of significance is expected to be high, but the definition remains ambiguous intentionally.

flows through the command and control to launch our massive retaliatory 2nd Strike, launch of delivery vehicles that can place warheads at targets, and finally concludes with the ability for warheads to ultimately destroy or incapacitate a target as described in Figure 10. However, because the vested interests of the authors and sponsors of this report are subject to warhead capabilities, science and technology, and effectiveness of nuclear weapons to hold targets at-risk, this detailed assessment provides the most detail for warhead subcomponents first, followed by delivery vehicles, and ultimately concluding with sensors and command and control.

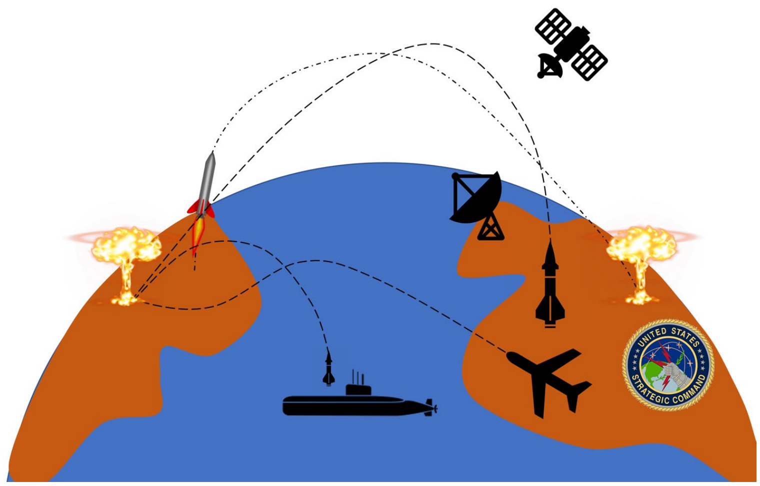

Figure 10: The critical sub-components of the secure second-strike tool to deter a massive first strike on the U.S. Assuming red launches a nuclear first strike on the U.S. homeland. The U.S. first needs sensors (e.g., radar facilities and satellites) to detect that a nuclear first-strike on the U.S. homeland is occurring, or has occurred, and who launched the attack. Then the U.S. needs the nuclear command, control, and communication (NC3; e.g., STRATCOM) to decide to respond with a strategic second-strike and communicate that order to the nuclear weapons delivery platforms. Then the nuclear warhead delivery vehicles (land: ICBMs, air: bombers, sea: SLBMs) must deliver the weapons to the adversarial targets. The final critical sub-component is the nuclear warheads that ultimately must impose a cost on the adversary. For each of these sub-components there are three key phases to the mission: deploy the sub-component capability, survive the first-strike, and impose cost on the target.

To develop a user interface that enables logical assessment of the technical credibility of the hardware to requirements as well as the implementation aspects we have organized this deterrence analysis capability into a logical matrix. A single component example of the matrix layout is shown in Table 2. This table contains the physical component as the major row category and can be further divided when necessary to specific hardware subcomponents for increased fidelity. Rows containing hardware details are then divided by each requirement supporting the mission phase. Each assessment of a component to a requirement is then split into sub-rows that enable discussion of current S&T as well as future minimum and future maximum S&T assessment and finally to trending discussions. Assessments are provided on a range of zero-to-one for S&T categories and from -1 to 1 for S&T trends. Justifications are then provided for evidence supporting the assessment.

Hardware	Phase	Range / Trend	Assessment	Justification
Component 1	Requirement 1	Current		
		Future Minimum		
		Future Maximum		
		Trend (-1, 0, 1)		
	Requirement 2	Current		
		Future Minimum		
		Future Maximum		
		Trend (-1, 0, 1)		
	Requirement 3	Current		
		Future Minimum		
		Future Maximum		
		Trend (-1, 0, 1)		

Table 2: The Deterrence Analysis tool, as developed in this report, provides the key and fundamental information to assess the state of a particular deterrence capability.

Once assessments are completed, they are graphed into a summary matrix that provides a clear snapshot of the assessment for dissemination as shown in Figure 11.

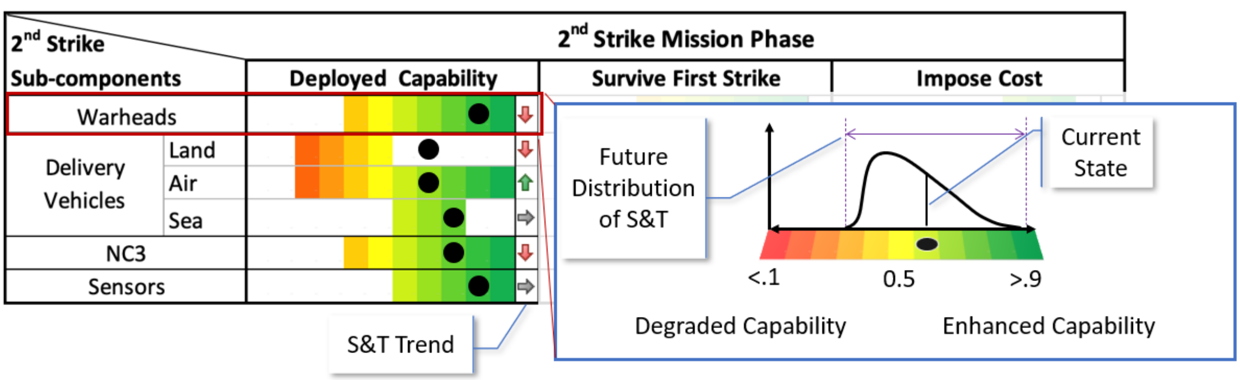

Figure 11: The assessment table "snapshot" matrix that provides all key assessment details as supported by the Deterrence Analysis tool.

Assumptions supporting Detailed Assessment of the Secure 2nd Strike Capability

To assure that logical conclusions are drawn from the following detailed assessment, the initial assumptions for our detailed assessment are outlined. While all assumptions could be debated within the scope of national security forums, it is important to set a baseline developed by our collective expertise within the national security and stockpile stewardship backgrounds. Assumptions are broken down between the requirements supporting the Secure 2nd Strike capability and the hardware or subcomponents necessary to realize a Secure 2nd Strike capability. This report relies exclusively on open-source discussions and publications and does not include or imply any classified knowledge is applied to this assessment. It is strongly recommended that interested parties review relevant sections and apply national security supported assessments in closed forums as necessary in future assessments.

Note that we have simplified our analysis by not considering the U.S. missile defense systems. We are focusing on deterring a massive nuclear first-strike through use of the Secure 2nd Strike and the current U.S. missile defense system would apply to a deterrence by denial strategy as compared to the deterrence by punishment strategy documented herein. As such, a U.S. anti-ballistic missile system would provide a highly effective and measurable influence upon the deterrence calculus for this scenario. However, to manage the expectations and variables within the construct and framework developed in this report, our focus on the Secure 2nd Strike deterrence tool is reasonable and helps to illuminate the specific methodology for how to assess a tool for deterrence effectiveness and simply acknowledge that within an integrated framework, missile defense would complement a Secure 2nd Strike.

Mission Kill-Chain Requirements

Deployed Capability

The first requirement for the Secure 2nd Strike capability is described as the deployed capability that represent the state of the component and hardware within the field as of the publication of this report. Included within this requirement is the implied product realization lifecycle and capacity to either replace or refurbish inclusive hardware.

Survive First Strike

The second requirement for the Secure 2nd Strike capability is the ability for subcomponents to survive the nuclear first strike action and represents the robustness of the hardware to be deployed within strike packages against targets-of-interest after the initial attack.

Impose Costs

The third requirement for the Secure 2nd Strike capability is the ability to effectively hold a target at-risk by destruction or incapacitation to an extent where further aggression cannot occur from that source.

Capability Realization Subcomponents

Warheads

Warhead assessments encompass the nuclear explosive and electronic systems supporting arming, fuzing, and firing of the warhead. Assessment interface are the mechanical and electrical interfaces to delivery vehicle systems. Included within this assessment are stockpile warheads such as the W80, B83 and B61, W87 and W78, and W76 and W88. It is also assumed that warheads are certified to military requirements for use.

Delivery Vehicles

Delivery vehicle assessments interface with warheads at the mechanical and electrical connection points of the warhead. Delivery vehicles are the primary mechanism to launch, carry, and deliver warheads to targets. Examples of inclusive delivery vehicles are the B-2 Stealth Bomber, tactical NATO fighters, and Air-Launched Cruise Missiles, Ohio-class SSBN and Trident II ICBMs, and Minuteman III ICBMs. It is assumed that delivery vehicles are certified to military requirements for nuclear use.

Nuclear Command, Control, and Communication (NC3)

The Nuclear Command, Control, and Communications (NC3) system encompasses the general infrastructure required to support NC3 capabilities such as National Security Cyber and Permissive Action Link (PAL) hardware that is required for authorization to use nuclear weapons. The President of the United States has the sole authority to authorize the use of U.S. nuclear weapons.

Sensors

The three primary roles sensors play in affecting the deterrence calculus related to deterring a first-strike on the U.S. with a secure nuclear weapons second-strike tool are: detecting a first-strike attack on the U.S. through land, radar, and space diagnostics, attributing that attack to the responsible adversary, and providing the information necessary to target the adversary assists with our nuclear second-strike force. In addition, this category of hardware supports quality assurance that warheads and delivery vehicles will operate as designed and planned within the context of the specific operational missions.

Assessment Criteria

Continuing the logic of deterrence calculus, we assess each sub-component based on its impact on the deterrence calculus. For this detailed case study, assessing how science and technology might impact the U.S. Secure 2nd Strike capability to deter a massive first-strike, while acknowledging but disregarding U.S. civil and missile defense, the deterrence calculus simplifies to considering the U.S. adversary's perceived cost being imposed on them by the U.S. if they should attack with a nuclear first strike, compared to the perceived cost the U.S. might impose even if they don't carry-out a first strike.

$$\frac{p(cost|action)}{p(cost|{\sim}action)} > 1$$

This report relies exclusively on open-source discussions and publications and does not include or imply any classified knowledge is applied to this assessment. It is strongly recommended that interested parties review relevant sections and apply national security supported assessments in closed forums as necessary in future assessments.

Current

Current assessment refers to the assessment of the science and technology implications of the subcomponent as it applies to the capability requirement as of the time of this writing.

Future Minimum

Future minimum refers to the assessment of science and technology assuming that our S&T capability is not effectively expanded or enhanced by our ongoing effort and that aggressor S&T progresses at a rate that is asymmetric to our current S&T efforts. We highlight where it also includes the possibility that we add S&T capability in one area that might have negative connotations in another. We consider an approximately ten-year time horizon.

Future Maximum

Future maximum refers to the assessment of science and technology assuming that our S&T capability is enhanced asymmetrically to adversarial or aggressor S&T development rates. We highlight where it also includes the possibility that we add S&T capability in one area that might have negative connotations in another. We consider an approximately ten-year time horizon.

Trend

The trend assessment gives an indication of whether we believe the current sub-component assessment is likely to hold in the future or trend towards the future minimum/maximum based on review, knowledge, and judgement of technological capabilities within the ten-year time horizon.

Sub-component Assessments

When reviewing hardware, the sub-components that support the mission requirements described in the previous section, we assess the current state, future minimum state, future maximum state, and trends with a focus on the science and technology supporting realization of the deterrence capability. The complete snapshot of the detailed qualitative assessments for this report is portrayed within Figure 12. Within the figure, the current state and future minimum/maximum range are represented by the solid black mark and colored scale, respectively. These assessments were scaled to a value between 0 and 1 in 0.1 increments, as our method for conveying our confidence within the assessment. At 0 (dark red), we assess the component may be unable to meet the detailed requirement and therefore may be unable to sufficiently support the deterrence capability as a whole within the calculus. Conversely, at an assessment of 1 (dark green), we have extremely high confidence in the component to meet the detailed requirement and contribute to a credible deterrence capability. Beyond the range portrayed in the figure (i.e., where no color exists in a given cell), we do not foresee any reasonable enhancements or degradations to that sub-component, thus inferring a non-applicability of the hardware to the requirement given the assumptions detailed above. It is important to note that while we may assess components as low and unable to sufficiently meet the detailed requirement, this does not imply immediate failure of the tool within the deterrence calculus. As noted previously, we have simplified the deterrence calculus to illustrate the effectiveness of this detailed assessment methodology. However, because of interacting and persistent correlations between the levers of deterrence, such as the absolute cost of an action relative to the probability that a cost for an action can be imposed, a trade-space between costs and benefits where action and inaction must be considered. These interactions are considered previously in the case study for the broad effectiveness of the nuclear weapon deterrence capability to the spectrum of adversarial actions.

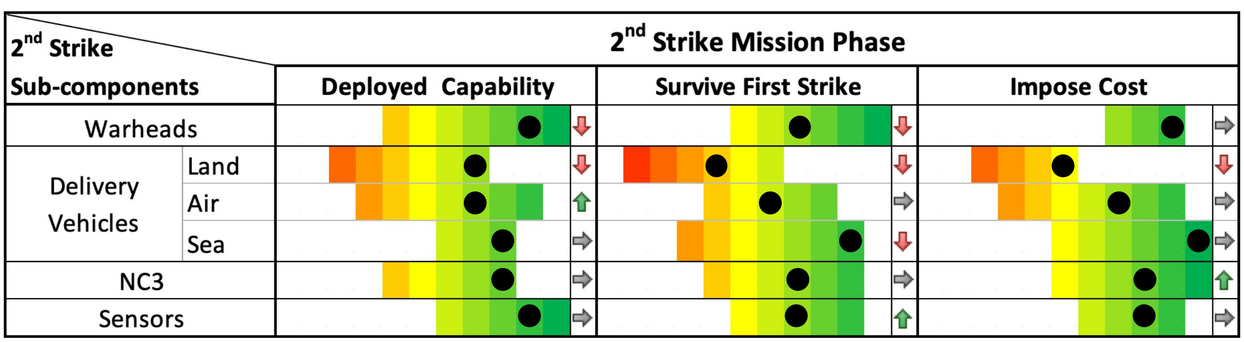

Figure 12: Snapshot of the overall detailed assessment for S&T Trends performed using the Deterrence Calculus Assessment methodology defined in this report. Markers define the current state of hardware capability with respect to the mission requirements. Future minimum and maximum are illustrated using a range of values from 0 to 1 where color coding represents the fidelity of this assessment (red towards zero, green towards 1). Arrows at the right side of each requirement column represent the trend in S&T as determined by this assessment.

In the subsequent discussions of this section, we analyze briefly the logic and evidence supporting our assessment for the science and technology snapshots and trends.

Nuclear Warheads

DEPLOYED CAPABILITY

Nuclear Warhead Assessment Summary	
Current	Warhead S&T include multiple yields for tactical and strategic options.
Future Minimum	Limiting factors include unique design requirements (e.g., no modularity), weapons are designed for incalculable lifetimes (e.g., exotic materials and long product realization timelines), and failure to mitigate known deficiencies (e.g., warhead STS limitations).
Future Maximum	The maximum S&T benefit for blue is self-imposed based on political motivation and S&T that accompanies the production to field lifecycle.
Trend	It is unlikely that warheads will be limiting factor in the near future. As warheads decay in the far future, this capability will eventually decline.

Current Justification

(0.9) Within the current strategic stockpile are a variety of warheads designed for specific delivery platforms that support all three legs of the nuclear deterrence triad; land, air, and sea. In general, robust processes are in place to ensure warheads are ready and fielded that meet reliability requirements. Fielded warheads have a variety of yields from low (kT) to high (MT) that enable a variety of response strategies, including the Secure 2nd Strike.

Future Minimum Justification

(0.4) The future minimum is dependent upon the need to produce new warheads as compared to recycling current warheads and is also a product of the current strategic posture of conflict (i.e., peacetime or conflict tensions). Recycling warheads is a minimal impact to current stockpile quantities with the exception that if warheads or warhead components cannot be recycled, the quantity decreases. The ability to produce "new" warheads and components is extremely difficult without political motivations based on the strategic security environment. For example, the ability to produce quality pits is currently under review, as is the ability to produce quality explosives to warhead defined specifications[64]. New warhead designs have not been adequately pursued for the U.S. stockpile since the 1990s and many key design skills have atrophied, including the loss of designer knowledge. Furthermore, the current warhead production infrastructure and process for fielding is inadequate, outdated, and substandard due to the friendly strategic security environment that did not emphasize a need for a robust nuclear deterrent. This has resulted in an approximate 5–10-year lead time from design to field readiness and will significantly impact warhead deployability in the future if not rectified. Commercial S&T is not applicable to destabilizing specific warhead capacity due to the weaponized nature of nuclear warheads.

Future Maximum Justification

(1) The future maximum depends on significant changes to the security environment or enhancement of national capabilities that enable production of "new" critical components (including the raw materials supporting design requirements), as well as continued recycling of warheads and components. The ability to create "modular" warheads is also another S&T mechanism that would enable the development of sufficient quantities of warheads that can be implemented and fielded in multiple different delivery systems within all legs of the triad, however, modularity requires significant and robust interface definitions between the warhead and the delivery platform. An additional S&T mechanism for ensuring warhead production can meet Secure 2nd Strike capability needs are changes to the lead-time required from design to fielding from the current 5—10-year estimate to 2—3-years. This can be accomplished by providing better definition of warhead lifetime requirements, robust safety and

[64] https://www.energy.gov/nnsa/plutonium-pit-production; accessed 3/5/2022.
See also: https://www.gao.gov/blog/2019/10/31/creating-explosives-for-nuclear-weapons; accessed 3/5/2022.

surety knowledge through empirical evidence and computational accuracy, and production throughput capacity that is commensurate to the quantity of weapons (tens to hundreds, not thousands). Maximizing our warhead capacity advantage is also relative to the political environment and support for a stockpile of nuclear weapons; political support for warheads is not discussed further in this assessment. Commercial S&T can also be leveraged by facilitating supply chain difficulties with enhanced rapid fabrication capabilities and increased efficiency in production and assembly methods.

Trend

(-1) The trend for warhead deployed capability is decreasing. While it is not convincing that the U.S. needs to adopt a relative measure of nuclear weapons instead of an absolute measure for the purposes of deterrence, the ability to defend against two simultaneous adversary problem impacts the quantity of weapons deployed. The inability to produce new warheads and lead-times approaching 10 years for modification of complex warheads exacerbates this challenge unless significant and sufficient changes to the warhead production infrastructure and the ability to produce "new" components and warheads can be pursued. Some mitigations to this trend can be implemented by developing "modular" warheads that can fit into multiple delivery platforms supporting different legs of the triad and also by re-defining warhead lifetimes to cycles that enable modest production and engineering development to allow focus on performance, reliability, and safety, rather than longevity.

SURVIVE FIRST-STRIKE

Current Justification

(0.7) Current survivability of warheads is well understood and studied by the NNSA National Laboratories (LLNL, LANL, SNL). These include limitations in the ability of warheads to survive in certain environments as defined through the Stockpile-to-Target Sequence (STS), of which, certain environments in the STS are applicable to survival of 1st Strike attacks.[65] There are also certain limitations related to specific material properties associated with aging phenomena. While known lifetimes of warhead materials, components, and sub-systems primarily impact the readiness of warheads, some key limitations may be stressed to failure by the 1st Strike environments and exacerbate the survivability of warheads through an attack to impose cost in the next mission phase.

Future Minimum Justification

(0.5) As adversaries develops more powerful, accurate, or disruptive weapon systems, our warheads will become more vulnerable due to exploitation (inadvertent and intentional) of known limitations. It is unlikely that red S&T will occur so swiftly that blue cannot adapt, however, the ability to counter red S&T development programs and field mitigating technology in modern warheads is challenging. Commercial S&T can potentially provide disruptive and detrimental influences by developing capabilities for weapons of mass destruction that mitigate nuclear effects or nuclear capabilities, but these capabilities are likely to be at the far horizon of this assessment.

Future Maximum Justification

(1) Development of our warhead S&T through knowledgeable resources and advanced materials or fabrication capabilities will enable new designs that meet future threat vectors and eliminate or mitigate

---

[65] Certification status of individual warheads is not readily available for academic purposes, however, it is expected that limitations or deficiencies exist due to the fact that numerous different types of warheads exist for different delivery platforms.

warhead vulnerabilities at the boundaries of our annually assessed reliability, thereby expanding the operational STS envelope. Incorporation of these technologies is usually slow and commensurate to the production/fielding lead-time, however, if coupled to advances elsewhere in the product realization lifecycle, significant gains in warhead design can be achieved rapidly with minimal impact to the development process. Additional gains may be realized by development of warheads with lifetimes commensurate to the quality of the "available" materials (i.e., materials are not exotic or extremely rare) whereby the replacement costs of warheads are significantly smaller than the development costs.

Trend

(-1) Trends for warheads to survive first strike attacks is decreasing due to the relative sluggishness in designing out known deficiencies in warhead designs that are approaching 40 years in the field. Incorporating modernized designs within fielded warheads over the course of multiple years that can meet or exceed the current STS envelope will mitigate this trend and ensure that adversarial knowledge does not encompass and bound our fielded design capabilities and limitations.

IMPOSE COST

Current Justification

(0.9) The current strategic warhead arsenal includes a variety of capable warheads with multiple yield options from low (kT) to high (MT) that enable a variety of response strategies including Secure 2nd Strike. In addition to the extensive testing programs that were conducted during the Cold War, the U.S. has devoted world-class efforts to stockpile stewardship and developed and refined capabilities to assure warhead reliability without the need for nuclear warhead testing. When coupled with delivery vehicle reliability and accuracy assessments, our warheads have the capability to impose significant cost through the range of security environments and operational theaters to hold significant targets at-risk.

Future Minimum Justification

(0.7) As adversaries develop increased anti-access/area denial (A2AD) capabilities, warheads may become less effective in their ability to couple damage to the designated targets due to hardening and other mitigating S&T such as shielding or other nuclear and physical effects, effectively decoupling the target from warhead outputs. Additionally, commercial S&T may enable disruptive and or detrimental technologies that mitigate the effects of nuclear weapons or become robust to nuclear effects. These commercial S&T endeavors may be enabled through concurrent development of advanced space vehicle technologies and commercial cyber-threat mitigations that can be inadvertently applied to nuclear technologies. Additionally, if the U.S. continues to decrease the quantity of warheads in our arsenal, the ability to field a massive 2nd strike is also diminished, however, any diminishment within the near future will be small due to the current quantity of warheads available.

Future Maximum Justification

(0.9) Our national S&T efforts for the cost imposed by nuclear weapons is approximately optimal, especially given the ability to field warheads of multiple yields and designs across a range of platforms. Significant enhancements could be gained by developing warheads that are designed to operate through a range of delivery vehicles across the nuclear triad as well as expansion of the warhead yield envelope to close the gap between conventional weapons and massive counter-value weapons that could destroy significant earth-protected structures within mountains or deeply buried and hardened targets.

Trend

(0) Trend is relatively flat but slightly decreasing due to the potential effect of increased adversarial A2AD capabilities and our lack of focus on designing and fielding mitigations to known stockpile limitations. Commercial S&T is not focused on weapon technologies and therefore it is likely to assume any disruptive commercial technologies would be accidental due to experimental activities in other fields.

Delivery Vehicles

Land

DEPLOYED CAPABILITY

Delivery Vehicles Land Assessment Summary	
Current	Limited by their ability to survive first strike, plus the haste associated with use-it-or-lose-it impetus negatively contributed to the deterrence calculus.
Future Minimum	The increasing pace of a potential conflicts and increase in the size of adversary arsenals is likely to further reduce the credibility of the land-based deterrent.
Future Maximum	Many of the technological steps that can be taken to improve the deterrent are countered by correlated $p(cost \mid {\sim}action)$ in the deterrence calculus.
Trend	Their vulnerability is only likely to increase in the future.

Current Justification

(0.7) The current U.S. ground-based nuclear inter-continental ballistic missile (ICBM) deployed capability is sufficient to ensure a Secure 2nd Strike capability is technically credible. Missile launch can be rapidly executed with delay limited only to the checks and balances for authorized nuclear use, regardless of time or target. The current U.S. ICBM force is well dispersed within the geographic locality. Modernization programs are currently underway and expected within the next decade. While the U.S. may not have enough missiles to fully absorb a first-strike, there are sufficient numbers such that the adversary must commit a large number of their force to destroy them, which produces high signal-to-noise ratio of their intentions. Additionally, the fact that the ICBM force is located on the continental U.S. implies that any debilitating attack on the ICBM force would likely increase the probably of the U.S. responding with a strong second-strike. The primary reason we don't assess this capability higher is that the ICBM vulnerability means that the U.S. must use them quickly in the event of a massive first-strike, which in turn increases $p(\text{U.S. nuclear weapon 2nd strike} \mid {\sim}\text{red nuclear weapon 1st strike})$ leading to instability and decreasing our deterrent effect.

Future Minimum Justification

(0.2) As China and other adversaries grow their stockpile it means that they can dedicate a larger fraction of their force to targeting our ICBM silos. Additionally, if we wish to maintain a flexible response strategy with the option for counter-force, then as we look to facing two near-peer nuclear adversaries as well as at least one minor adversary we may not have a sufficient number of ICBMs to maintain the current strategy, especially if our adversaries increase the number of weapons in their stockpile. As the operating environment becomes more complex with even more nuclear powers it will strain our decision making increasing the perceived adversarial calculus assessment of $p(\text{U.S. nuclear weapon 2nd strike} \mid {\sim}\text{red nuclear weapon 1st strike})$, degrading our overall deterrent further. This is further lowered due to the lack of replacement capabilities. Next generation platforms, such as the Ground Based Strategic Deterrent (GBSD) are still many years away from first production unit (FPU) or initial operating capability (IOC). Lead time for delivery systems is many years, likely decades and will require consistent funding and advocacy through multiple political administrations.

Future Maximum Justification

(0.7) S&T can support the future maximum through improvements in missile-to-warhead interfaces (i.e., development of standardized deployment packages), re-implementation of multiple independent re-entry vehicle (MIRV) capabilities to enhance the number of targets a single missile can deploy against, as well as targeting multiple warheads against a single target with advanced A2AD, and finally by adding additional warhead/missile geographic dispersal to ensure the capability maintains widely dispersed characteristics. All of which increase $p(\text{U.S. nuclear weapon 2nd strike}|\text{red nuclear weapon 1st strike})$, and favorably improve the deterrence calculus. That said, even if we address the supply chain and human resource issues enabling us to build more capable ICBMs in a manner more efficiently than our adversaries, the problem remains that our ICBM force is vulnerable because it is a static launch point. This in turn will drive us to make quick decisions if we wish to use them which will keep the perceived $p(\text{U.S. nuclear weapon 2nd strike}|\sim\text{red nuclear weapon 1st strike})$ relatively high and thus limit how effective this deterrent will be. Furthermore, if we build a larger ICBM force to counter their vulnerability it will also drive $p(\text{U.S. nuclear weapon 2nd strike}|\sim\text{red nuclear weapon 1st strike})$ higher.

Trend

(-1) This trend is decreasing rapidly due to the lead time required make available a deployment-ready modern missile capacity and capability coupled with the general increased complexity of the operating environment with more capable NW adversaries. In addition, general international competition is driving the system into a state where it is difficult to maintain sufficient capability with our ICBM force. Furthermore, their vulnerability is only likely to increase and thus drive us to an operating procedure that is likely to further increase $p(\text{U.S. nuclear weapon 2nd strike}|\sim\text{red nuclear weapon 1st strike})$ if we wish the force to be effective in imposing cost, but this dynamic is counterproductive.

SURVIVE FIRST-STRIKE

Current Justification

(0.4) The ground-based systems are geographically distributed across a wide range of territory requiring significant numbers of adversarial first-strike weapons to account for all potential targets. Additionally, silos are generally robust (but not immune) to low-order first-strikes and conventional munitions, meaning destruction of the capability requires nuclear first-strikes to be efficient. Furthermore, launch-time requirements from silos is fairly short, meaning that presidential authorization, once given, can be executed swiftly and mitigate much damage that could be done if verification of silo-targets-prior-to-impact is obtained by our sensor indication and warning (I&W) capabilities. The launch on short notice capability is counter-productive to some degree because it increases $p(\text{U.S. nuclear weapon 2nd strike}|\sim\text{red nuclear weapon 1st strike})$.

Future Minimum Justification

(0.1) The future minimum is dependent upon the ability of adversaries to field/deploy greater numbers of weapons, with increasing power and accuracy. This includes hypersonics that shorten response time or warheads with greater efficiencies to couple nuclear energy into ground phenomenology and damage launch infrastructure. Coupled with the increased urgency in ‘using or losing’ the U.S. ICBM will increase $p(\text{U.S. nuclear weapon 2nd strike}|\sim\text{red nuclear weapon 1st strike})$ and further degrade U.S. overall deterrent. Commercial technologies will likely enhance targeting accuracy as well as other detonation characteristics/parameters such as Height-of-Burst (HOB) accuracy that will enhance adversarial target-to-kill ratios.

Future Maximum Justification

(0.6) With improved sensors and I&W it is possible that we might more confidently launch our ICBMs before they are destroyed. It is difficult to conceive increasing this significantly though since the primary means is by increasing the number of ICBMs and this can easily be offset by our adversaries additionally increasing their number of nuclear weapons, potentially leading to an arms race. Enhancement and co-location deployment of missile defense systems may temporarily help, but this could be easily countered by our adversary since offensive and decoy capabilities are much cheaper than missile defense. If the missile defense was co-located and had very limited range capability it is possible to increase $p(\text{U.S. nuclear weapon 2nd strike}|\text{red nuclear weapon 1st strike})$ without inadvertently increasing $p(\text{U.S. nuclear weapon 2nd strike}|{\sim}\text{red nuclear weapon 1st strike})$. It is possible to reinforce existing silo/launch infrastructure to harden against increased adversary strike power, however this may be countered with increased adversary numbers, power, and accuracy. Finally, advancements in commercial materials technology may also enable mitigation of adversarial nuclear effects by increasing missile robustness.

Trend

(-1) We believe this is trending flat to negative. The largest negative driver is that U.S. adversaries are increasing their number of ICBMs and/or modernizing their existing force making the U.S. ICBM force more vulnerable, coupled with the challenges of establishing/maintaining favorable arms control agreements.

IMPOSE COST

Current Justification

(0.5) The ability to impose cost from U.S. ground-based systems with a Secure 2nd Strike is immense. Ground-based systems have high confidence in target accuracy with an overwhelming number of missiles and warheads. Warheads can be launched rapidly with independent warheads prosecuting the same target to ensure damage is maximized. This is somewhat limited by their ability to survive a first-strike. While this can be overcome by I&W from the sensor sub-component and the rapid launch capability, this is countered somewhat by the increased perceived $p(\text{U.S. nuclear weapon 2nd strike}|{\sim}\text{red nuclear weapon 1st strike})$ resulting from the need to make a hasty decision.

Future Minimum Justification

(0.2) While the future minimum is somewhat dependent on the U.S. adversary's ability to field ABM capabilities, it is more limited by the vulnerability of the U.S. ICBM force (given that offense is cheaper than defense; driving perceived $p(\text{U.S. nuclear weapon 2nd strike}|\text{red nuclear weapon 1st strike})$ lower) and the negative coupling of this fact driving the U.S. to make a hasty presidential decision of 'use it or lose it' which drives the perceived $p(\text{U.S. nuclear weapon 2nd strike}|{\sim}\text{red nuclear weapon 1st strike})$ higher. U.S. adversaries can also potentially reduce the number of viable warheads and impose a limiting factor in the ability for ground-based systems to impose cost; for example, launch disruption technology through cyber, mechanical, or electromechanical means. Commercial S&T may play a key role in developing instabilities in ground-based strategic deterrence due to advances in materials associated with re-entry capabilities, maneuverability of ABM/A2AD, and autonomous swarm technologies (i.e., drone swarms) that could enhance adversary A2AD.

Future Maximum Justification

(0.5) While the U.S. can enhance its probability of imposing a cost with its ICBM force by increasing boot-phase and maneuvering capabilities, as well as enhanced decoy capabilities, all to overcome adversary missile defense systems, these systems are relatively limited currently and not likely to be invested in heavily in the future (due to defense being significantly more expensive than offense). Thus, the future maximum will ultimately be limited by the U.S. ICBM force's vulnerability. The U.S. can attempt to compensate for the vulnerability of its ICBM force and increase $p(\text{U.S. nuclear weapon 2nd strike}|\text{red nuclear weapon 1st strike})$ by increasing the number of missiles. However, this could be compensated for by the adversary increasing its nuclear weapon force. Furthermore, it would be somewhat counterproductive by increasing the perceived $p(\text{U.S. nuclear weapon 2nd strike}|{\sim}\text{red nuclear weapon 1st strike})$. While commercial S&T, specifically related to materials stabilized for atmospheric re-entry, can also improve the capability of U.S. ground-based systems to impose cost, this is not the limiting factor.

Trend

(-1) This is primarily driven by the U.S. ICBM ability to survive a first strike, as adversaries increase their number of nuclear weapons and their capability, and the U.S.'s limited ability to counter this without appearing unintentionally threatening of imposing a first-strike itself.

Sea

DEPLOYED CAPABILITY

Sea-based Nuclear Weapon Capability	
Current	Contributes to S&T instability due to its ability to move virtually undetected throughout the world's oceans and creates incentives to develop technologies that can track deployments and asset locations.
Future Minimum	Future minimum is governed by disruptive effects through exploitation of networks creating "trip-wires."
Future Maximum	Future maximum is governed by blue's ability to remain clandestine through sea operations in all phases of deployment.
Trend	Overall trend is remaining constant due to the difficulty and lead time that would be required to either create any new S&T (Blue or Red) or the lead time required to exploit any vulnerabilities in commercial S&T efforts.

Current Justification

(0.8) While the SLBMs make up a minority of our strategic force, current capacity is sufficient for threatening to impose massive retaliation to nuclear 1st strike aggression in a swift and reliable manner. The ability to maintain the current fleet and strategic needs are assessed through production capacity and modernization program implementation. With respect to production capacity, lead times for submarine fabrication is very predictable. Additionally, modernization programs are underway for the next generation of strategic nuclear-armed submarines (Columbia Class), however, the development and IOC timeframe is significant and approaching two-decades from concept to IOC.

Future Minimum Justification

(0.6) The future minimum assessment for deployed capability is based on concern about two near peer nuclear adversaries and if we have sufficient assets to hold targets of both adversaries at risk simultaneously. The future minimum is governed by our national commitment to continuity of asset development and production schedules given multi-decade (multiple administration) lead times. However, the future minimum is not heavily dependent on S&T development by adversaries because asset development and production schedules are a function of politics and raw materials. On the other hand, commercial S&T sources may provide disruption to future minimum by limiting available resource quantities or development of processes that highlight vulnerabilities and weaknesses in fabrication and assembly.

Future Maximum Justification

(0.8) The future maximum assessment for deployed capability is based on the anticipated strategic SSBN force size and governed by our ability to significantly shorten and mitigate lengthy lead times for product realization and IOC. Commercial S&T could provide major influence in fabrication and assembly methods and processes if the technology can be incorporated into many different system lifecycle phases. Influences from commercial S&T span the range between enhancements in metal-alloy properties, to advanced alloy fabrication, enhanced raw-material production, and improved weld and assembly techniques.

Trend

(0) Trends for sea deployed capacity is flat or potentially slightly increasing due to challenges that are politically-motivated resource constraints or based on commercial S&T technologies that will hopefully be incorporated in asset lifecycle phases rather than overlooked or ignored. There is a distinct lack of major disruptive adversarial S&T influencing this trend.

SURVIVE FIRST-STRIKE

Current Justification

(0.9) The ability for the sea-leg of the U.S. nuclear triad to survive first strike is very good and creates significant advantage for the U.S. strategic deterrent. SSBN submarines can largely remain undetected throughout the world's oceans and are relatively uncontested in strategic posturing and positioning. Adversarial A2AD is largely insufficient to prevent or preclude our sea assets from operating within strategic strike areas of operations and have limited abilities detecting assets as they can only be detected when they are within the immediate area of observation or if human errors are committed by our strategic forces. Commercial S&T has not developed any specific leverage or vulnerabilities to exploit at this time.

Future Minimum Justification

(0.3) Future minimum for sea-leg survival of a nuclear 1st strike is based on the ability to remain undetected within an area of strike capability and throughout operational mission phases. Aggressor A2AD capabilities must be significantly improved and expanded to create significant risk, however, this type of S&T is likely to be pursued due to its extremely disruptive influence. Significant technologies include the ability to detect or track SSBNs through enhanced sonar networks, leveraging oceanic displacement, or identification of radiation fields through light or material interactions. Commercial S&T is likely to be disruptive to our strategic deterrent capability through enhancements to nominal scientific endeavors and research related to mineral and biological exploration ventures. These ventures may create "trip-wire" like networks of sensors that could be exploited to track movement and posturing of our deterrence assets in operational theaters.

Future Maximum Justification

(0.9) Future maximum is incumbent on maintaining SSBN stealth capability but also based on having the correct quantity of operational assets deployed at a given time. Enhancing SSBN stealth technologies can be performed through enhanced materials research, robust operational techniques and procedures, developing ability to launch at deeper depths to avoid detection during launch phases, and shielding of detection signatures. In terms of sheer quantity, having a greater number of SSBNs on patrol at any given time will certainly increase the likelihood of survival, however, this increase may also unintentionally upset or imbalance conflict stability/instability, thereby increasing the cost of aggressor inactions within the deterrence calculus.

Trend
(-1) The trend for SSBN survival of an adversarial first strike is moving toward decreasing, but at a slow rate. It is not clear that we will be able to improve submarine technology at a faster rate than our adversaries can deploy more sensors and develop new detection technology. One challenge is that our adversaries are likely to know how well they can track our subs before we know how well they can track them, producing an asymmetric disadvantage. As an additional source of potential disruption, commercial S&T efforts must first create a vulnerability and then be exploited by our adversaries prior to effectively decreasing our SSBN capability to survive.

IMPOSE COST

Current Justification
(1) The ability for our strategic submarine nuclear force to impose cost is a strong cornerstone of the strategic deterrence against adversarial first strike due to the ability to covertly and rapidly retaliate with limited to no notice from any Area of Responsibility (AOR). Our SSBN capacity allows significant advantage with only a small window of vulnerability. Our nuclear strategies enabled by both moderate-to-high-yield and low-yield options provide flexibility in holding adversarial targets at-risk. Limitations are generally governed by availability of manpower resources and human competence in mission execution.

Future Minimum Justification
(0.5) The future minimum for the SSBN capability to impose cost is governed by the ability to survive first strike and the total strategic yield of each asset as defined by political negotiations through treaties. Manpower resources and human competence in mission execution are key elements that may also be exploited by aggressor S&T where complex counter-operational tools may strain our resources and tactics for a given AOR through fatigue and high operations tempos. Additionally, disruptive commercial S&T could be a factor if vulnerabilities in production and fabrication can be exploited by aggressors and limit the operational capacity at any given time.

Future Maximum Justification
(1) The future maximum can be enhanced through mitigation of potential vulnerability elements including remote or autonomous navigation and scaling size of platforms to decrease the footprint of detection. Additionally, it is conceivable that we could increase the damage that each SLBM warhead could inflict. Also adding more SLBMs to our force might increase costs imposed on aggressors, but also might unintentionally increase adversarial costs for inaction making the overall deterrence capability of the SSBN force less effective by increasing conflict instability.

Trend
(0) Trends for the ability of the SSBN nuclear forces to impose costs are flat based on the yield effectiveness of the sea-leg capacity and the lack of detection capabilities. By continuing to develop our

S&T efforts and increase autonomy or decrease detection footprints, we will maintain strategic advantage for long-term deterrence.

Air

DEPLOYED CAPABILITY

Current Justification

Air-based Nuclear Weapon Retaliation Capability	
Current	Current Air delivery systems are credible, but no longer serve on alert – this is a disadvantage if a surprise attack were observed.
Future Minimum	Not updating the current systems could leave this leg of the triad somewhat short as adversaries advance A2AD technologically.
Future Maximum	Current modernization is underway and should be sped up in order to keep this deterrent strong.
Trend	The overall trend is flat due to the speed of modernization.

(0.7) Air delivery systems include the U.S. bomber fleet. While some Fighter planes can deliver gravity nuclear weapons, the range and number of weapons that are deliverable are limited. The B-52H has the capability to deliver air launched cruise missiles. The B-52H and the B-21 (expected in the near future) strategic bombers are well suited for most situations that the US would face, either from a launch by the adversary or for a major conventional war abroad. In addition they signal U.S. support to the allies, if adversarial invasion comes to pass. “Bombers are the only triad leg to provide substantial conventional capabilities.”[66] The B-52 is one of the USAF’s workhorses. These planes, which became operational in 1955, have continually been upgraded and are expected to remain in service until 2040 and beyond. As of June 2021, the payload capacity for the B-21 Raider had not been released. The requested fleet is for 100 aircraft. The B-21 is expected to have capabilities that dominate globally and will feed into the future trend/capabilities.

	F-15-E	F16A/B/C/D	PA-200	B-2A	B-52H
B61-3	X	X	X		
B61-4	X	X	X		
B61-7				X	
B61-11				X	
B83-1				X	
AGM-86B/W80-1					X
B61-12	X	X	X	X	

Figure 13: The current arsenal allows for gravity bombs to be carried by the fighter plans listed in green and air launched cruise missiles are

The current air fleet has an advantage over ballistic missiles that the nuclear weapons can be recalled after launch, thus it may not increase p(cost|~action) as much as ICBMs do (less haste). That said, a distributed force still exists and thus the chances of accidents increases (thus p(cost|~action) increases, decreasing the effectiveness of this deterrent somewhat).

Several types of air-delivered systems currently exist with sufficient capacity and capability to enable Secure 2nd Strike destruction, including gravity bombs and air-launched cruise missiles. Air delivered systems provide the Commander-in-Chief the unique position to employ stealth delivery technologies as

[66] “Nuclear Force Posture and Nuclear Command, Control, and Communications” – Proportionate Deterrence: A model Nuclear Posture Review, Carnegie Endowment, January 21, 2021

well as enhanced tactical stand-off within the battlefield. Sufficient capacity is currently fielded as a robust leg of the triad. Current modernization programs are underway, however, it is still expected to be at least a half-decade to full-decade before IOC. Range for air-delivered systems is minimal with standoff capabilities being in the low thousands of km and gravity systems being subject to the penetrability of the delivery aircraft.

Future Minimum Justification

(0.3) With continued investment by our adversaries in A2AD and no clear efficient major opportunities for the US to counter those systems, it seems quite possible this force will become a less effective deterrent of a NW first strike on the US with time. (However, it may remain valuable to deter other actions.) [67]

Future minimum is dependent upon the capability of red A2AD to defend against stealth delivery platforms. Stealth detection capabilities have been an S&T effort since the introduction of stealth technologies in fighters and bomber aircraft in the 1980s and are expected to improve in the coming decades with new sensor technologies that can interpret signatures with increased complexity in significantly less time. Commercial S&T will likely accelerate detection sensor development through the drive to develop autonomous systems (for example, the advancement of self-driving vehicle technologies that incorporate multi-modal signature analysis to detect environmental conditions on roadways).

Bombers have some downsides to include adversarial advances in A2AD technological defense, and additionally, none of the bomber fleet is on alert, making it very difficult to respond quickly if an adversarial launch is detected. Bringing back a portion of the alert force would help greatly. In addition, it may be necessary to consider reopening some of the bomber bases that were closed during the 1990s. As it stands, if we chose to do nothing to counter adversarial advances, and leave the alert force off the table, we could be at a significant disadvantage in responding to an adversarial first strike.

Future Maximum Justification

(0.9) It is possible to switch to an always on alert posture to minimize the number of bombers that might be destroyed in a first strike attack, however there is still the A2AD problem to deal with. We could invest heavily in hypersonics to more effectively take out our adversary's A2AD systems, as well as the necessary intelligence network for targeting these systems.

Future maximum of air-delivered weapon systems is coupled to two abilities; penetrability (stealth) and standoff (range). Ability for blue S&T to decrease delivery platform signatures across the UHF and long-wave spectrums will be key to maintaining stealth capabilities. Additionally, standoff ability should be pursued for weapons to be fired as soon as possible, with full control up until target prosecution, ideally from ranges outside of defense platforms or farther. Commercial S&T will certainly aid to this through networked systems that allow control of autonomous vehicles beyond the horizon as well as new fuel platforms that may not require re-fueling but significantly enhance range capabilities.

---

[67] RAND analyst David Ochmanek has stated that the Blue (the U.S. and it's allies) would suffer heavy losses in scenarios where Blue is needed to defend the Baltics or Taiwan. It is also noted that unless the F-35 is in flight, it is easily destroyed (in large numbers) while on the ground. Breaking Defense, https://breakingdefense.com/2019/03/us-gets-its-ass-handed-to-it-in-wargames-heres-a-24-billion-fix/

The future max of the deployed capability would include a full B-21 Raider force alongside a stout, refurbished B-52 force. While it is unlikely that the US would be surprised by an unpredicted adversarial launch, both of the bomber forces will need to engage in some level of alert activity in order to maintain survivability. In addition, it is recommended that a couple of the previously closed bomber wings re-open to provide additional alert support in case of a global conflict.

Trend

(1) The current trend is increasing due to the ability leverage bulk technologies that benefit the capability of air-delivered platforms. The major limitation of the air-delivered platforms is the ability of planes and cruise missiles to remain stealth and launch from over-the-horizon. However, commercial S&T is helping to solve these challenges for industrial use, therefore, leveraging this technology as it becomes available will be key to maintaining an increasing trend.

The United States is on track to acquire 100 B-21 Raider bomber planes. The advanced capabilities of these planes is expected to put the country at an advantage over the adversary as the planes are not only nuclear capable, but also conventionally enabled.

SURVIVE FIRST-STRIKE

Current Justification

(0.6) The ability to survive a first strike for air-delivered systems is limited due to the lead time to launch aircraft. While STRATCOM, during the height of the Cold War, had aircraft on alert status for rapid launch in addition to aircraft in the skies on a continuous basis, the current posture is not accommodating of such rapid deployment. Vulnerability of air-delivered fleet is dependent upon the size, caliber, quality, and accuracy of red first strike.

A portion of the bomber fleet would likely be able to take flight if informed of an adversarial first strike launch. This would likely be limited to the teams that were conducting exercises on base and those that were readily available for deployment. A portion of the fleet would remain flightless and likely not survive a first strike. It is for this reason that a partial return of the alert force is recommended for future operations.

Future Minimum Justification

(0.4) As red develops increased or enhanced first strike capabilities, including hypersonic platforms and increased stealth S&T, the ability for air-delivered systems to survive first strike will diminish without changing CONOPS posturing and enabling robust mitigations against red targeting strategy. Commercial S&T is likely to be a double-edged sword in terms of both future minimum and future maximum by enabling better materials that can be leveraged for stealth applications as well as platforms and materials that facilitate hypersonic delivery. Both hypersonic and increased number of Chinese ICBMs will have negative impacts for our bomber force being able to get airborne in the event of a first strike.

Future Maximum Justification

(0.8) It is possible to switch to an always on alert posture to minimize the number of bombers that might be destroyed in a first strike attack. Additionally, improved sensors and I&W can also improve the survivability of this force. In addition, even a smaller, partially enabled alert force, would positively impact the reaction time in getting the bombers in flight prior to destruction by adversarial first strike.

Other blue S&T recommended to increase future maximum is dependent upon the ability for blue to launch weapons earlier from farther distance away from the target without the chance of detection. This implies that blue must have a robust S&T program in cooperation with commercial entities that also have a vested interest in similar technologies as outlined previously.

Trend

(0) With improved sensors and I&W it is possible that we might increase the probability of launching our bombers before they are destroyed in a first strike attack. If our adversaries start to arm hypersonic weapons with nuclear warheads this may counter this improvement.

While no specific S&T threat exists at present, it is also generally easier to target airfields with multiple planes that carry multiple warheads rather than trying to defend against an individual plane carrying the treaty-allotted nuclear armament. The ability to geographically and spatially separate planes and warheads will continue to be a challenge for blue.

As partial mitigation, new technology is being developed to detect hypersonic systems. In the advent of this development, the response time for bombers to take flight will increase. In addition, it is recommended that a portion of the alert force returns; possibly 50-70 percent of the cold war era force would return.

IMPOSE COST

Current Justification

(0.7) Air delivered capabilities to impose cost is coupled to two abilities; penetrability (stealth) and standoff (range). Both abilities are well developed and utilize the latest technological advances to ensure maximum risk is imposed against enemy targets. Current capabilities are limited by red A2AD capabilities that are inferior, but not incompetent, and it is unclear how effective these A2AD capabilities will be if they are "on alert" after a first strike volley. While STRATCOM assessments of current capabilities are not readily available, it is assumed that next generation delivery platforms (B-21 and LRSO) will fill the gaps and needs for continued effectiveness with minimal losses and continue to hold targets at risk. When assured that assets are airborne and ready to deliver payloads, the standoff capability of our B-52H and the future capability of the stealth B-21 Raider will ensure that the air-delivered Secure 2^{nd} Strike is imposed.

Future Minimum Justification

(0.3) Future minimum is dependent upon the ability for red to field/deploy advanced A2AD and stealth-mitigating technologies. Active development of these technologies will limit the effectiveness of significantly degrade blue capability. Commercial S&T is likely to progress faster than government S&T due to market forces that will enable advanced materials, airframes, and commercial transport capabilities that provide incentive for corporate expansion. Furthermore, if the United States does nothing to update the bomber fleet and bring back a portion of the alert force, then the survival of a first strike may not be detectable and very few bombers in the fleet would be ready to take flight until it was too late.

Future Maximum Justification

(0.9) Continual development of stealth technology along with hypersonics and new capabilities will give the United States a significant advantage. The developmental timeline for major nuclear modernization programs is shown in Figure 14 below[68]. If we invest in hypersonics and other anti-A2AD capabilities, then our strategic bomber force could increase credibility in terms of the deterrence calculus to impose costs for the adversarial action. Future maximum can also be enhanced through advances in spatial regimes above (spatially) and beyond (range) current capabilities. The ability to deliver weaponry from altitudes above the range of current air defense systems or launch weapons from over the horizon will maximize the targets at risk and effectiveness of blue to impose cost.

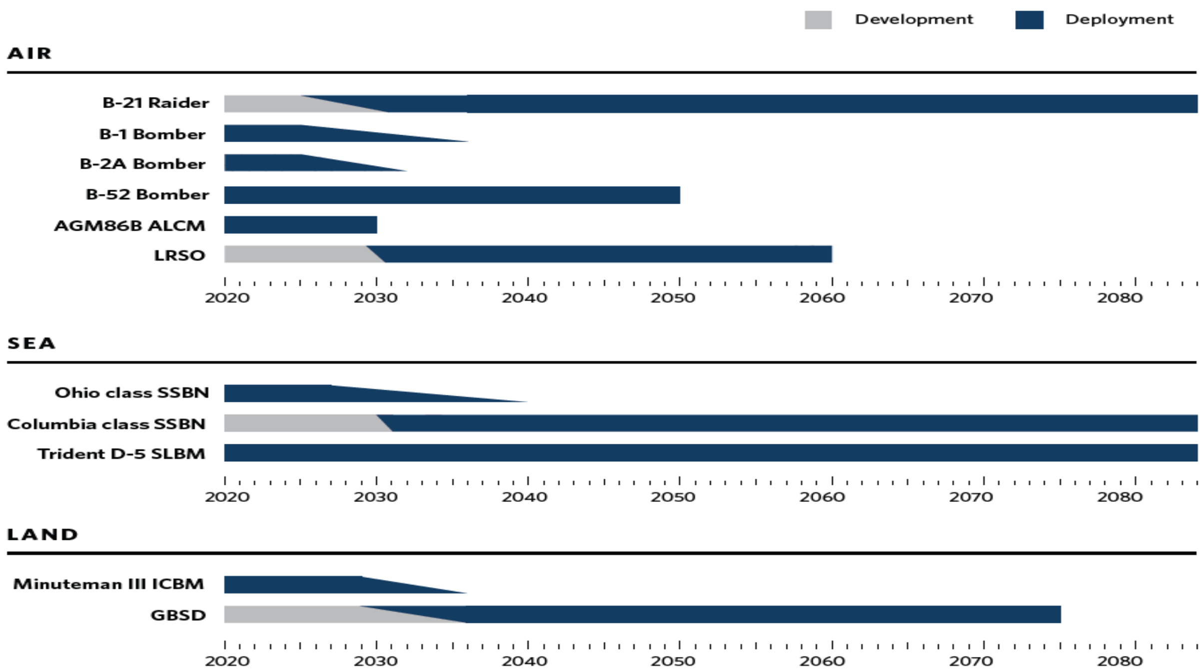

Figure 14 Borrowed from Percovich and Vaddi's Proportionate Deterrence and compiled from many sources.[69] Illustration of timeline for major nuclear modernization of U.S. capabilities, as currently planned.

---

[68] From Perkovich and Vaddi's Proportionate Deterrence – with additional references: Sources: Hans M. Kristensen and Matt Korda, "United States Nuclear Forces, 2020," *Bulletin of the Atomic Scientists* 76, no. 1 (2020); Ronald O'Rourke, "Navy Columbia (SSBN-826) Class Ballistic Missile Submarine Program: Background and Issues for Congress," R41129, Congressional Research Service (updated October 7, 2020), https://fas.org/sgp/crs/weapons/R41129.pdf; Tyler Rogoway, "USAF's Controversial New Plan to Retire B-2 and B-1 Bombers Early Is a Good One," The Drive, February 12, 2018, https://www.thedrive.com/the-war-zone/18410/usafs-controversial-new-planto-retire-b-2-and-b-1-bombers-early-is-a-good-one; Amy F. Woolf, "U.S. Strategic Nuclear Forces: Background, Developments, and Issues," RL33640, Congressional Research Service (updated December 10, 2020), https:// crsreports.congress.gov/product/pdf/RL/RL33640/65; Kingston Reif, "U.S. Nuclear Modernization Programs," Arms Control Association, August 2018, https://www.armscontrol.org/factsheets/USNuclearModernization; Megan Eckstein, "Navy Beginning Tech Study to Extend Trident Nuclear Missile Into the 2080s," USNI News, November 14, 2019, https://news.usni.org/2019/11/14/navy-beginning-tech-study-to-extend-trident-nuclear-missile-into-the-2080s.

[69] Sources: Hans M. Kristensen and Matt Korda, "United States Nuclear Forces, 2020," *Bulletin of the Atomic Scientists* 76, no. 1 (2020); Ronald O'Rourke, "Navy Columbia (SSBN-826) Class Ballistic Missile Submarine Program: Background and Issues for Congress," R41129, Congressional Research Service (updated October 7, 2020), https://fas.org/sgp/crs/weapons/R41129.pdf; Tyler Rogoway, "USAF's Controversial New Plan to Retire B-2 and B-1 Bombers Early Is a Good One," The Drive, February 12, 2018, https://www.thedrive.com/the-war-

Trend

(0) Trend for air-delivered systems to impose cost is flat due to the active modernization programs (B-21 & LRSO) and the uncertainty of commercial S&T to deliver products that would significantly challenge the ability for delivery platforms to hold targets at risk. However, there is a slight bias towards negative trends because our adversaries are investing heavily in A2AD capabilities, and at a rate faster than we are investing in capabilities to enhance our bomber force to overcome their A2AD.

NC3

DEPLOYED CAPABILITY

Current Justification

Nuclear Command, Control, and Communications Summary	
Current	It is understood that the adversary continues to develop and seek disruptive capabilities (such as Cyber) to impact current NC3 systems. Replacing the current system would be the best option as the old systems are vulnerable.
Future - Minimum	Many of the systems within NC3 are antiquated and need replacement. If nothing is updated, this capability will be greatly impacted.
Future Maximum	There are plans to modernize the NC3 system, but these plans cost money. The cost to maintain and replace these systems are around $79B
Trend	Some plans and advances have been made in updating these systems, but it isn't clear that they're on track and on budget.

(0.8) United States nuclear command and control is designed to enable the President of the United States, as the sole authority to launch the U.S. nuclear weapons against an adversary, without exception. The President does not require authorization from any other body of government and neither Congress, nor the military can overrule his orders if a decision to launch is made. According to DoD's Nuclear Matters Handbook, the elements of the nuclear command and control system "support the President, through his military commanders, in exercising presidential authority over U.S. nuclear weapons operations.[70]" The system relies on "a collection of activities, processes, and procedures performed by appropriate military commanders and support personnel that, through the chain of command, allow for senior-level decisions on nuclear weapons employment." Specifically, the nuclear command and control system provides the President "with the means to authorize the use of nuclear weapons in a crisis and to prevent unauthorized or accidental use."' Nuclear command and control systems communicate information related to the threats to the United States as collected through our national intelligence apparatus. The command-and-control systems also aid in advising the President on response options and communicates the options chosen by the President to the forces in the field.

The employment of our nuclear arsenal is only as reliable as the command, control, and communication systems that manage it. To assess the criteria that ensures this viability, we review the effective monitoring and control of all the nuclear forces in every rationally predicted scenario. NC3s ability to provide timely warning of adversarial nuclear launch is assessed. It is assumed that within these

---

zone/18410/usafs-controversial-new-planto-retire-b-2-and-b-1-bombers-early-is-a-good-one; Amy F. Woolf, "U.S. Strategic Nuclear Forces: Background, Developments, and Issues," RL33640, Congressional Research Service (updated December 10, 2020), https://crsreports.congress.gov/product/pdf/RL/RL33640/65; Kingston Reif, "U.S. Nuclear Modernization Programs," Arms Control Association, August 2018, https://www.armscontrol.org/factsheets/USNuclearModernization; Megan Eckstein, "Navy Beginning Tech Study to Extend Trident Nuclear Missile Into the 2080s," USNI News, November 14, 2019, https://news.usni.org/2019/11/14/navy-beginning-tech-study-to-extend-trident-nuclear-missile-into-the-2080s.

[70] Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, "Nuclear Matters Handbook." Revised 2020. https://www.acq.osd.mil/ncbdp/nm//NMHB2020rev/

scenarios, NC3 provides timely warnings in addition to situational awareness. We also assume secure and effective communications within the national command. Within this infrastructure, it is also assumed that the required secrecy in working with the nuclear stockpile is maintained.

The Advanced Extremely High Frequency (AEHF) constellation is a group of communications satellites that provides both tactical communications (i.e., for conventional forces like Army brigade combat teams) and strategic communications (i.e., for nuclear forces). AEHF, first launched in August 2010, replaced the Miltstar constellation from the 1980s. Paired with the Family of Beyond Line-Of-Sight Terminals (FAB-T), AEHF provides assured communications to nuclear forces like the Minuteman III intercontinental ballistic missile, the B-2 Spirit, and the E-4B National Airborne Operations Center. The Space Force has begun developing a new series of communications satellites called the Evolved Strategic Satellite (ESS) program.[71]

Future Minimum Justification

(0.4) China and Russian military strategists and planners focus on countering adversaries' command, control, communications, computers, intelligence, surveillance, and reconnaissance capabilities. A central focus is striking critical targets to paralyze an adversary's military ability and political willingness to sustain a fight. As the systems grow more complex there will be a larger infrastructure available for our adversaries to attack with cyber tools. Additionally, the advent of quantum computing and associated decryption might make even our secure networks venerable. In a recent Congressional Research Service report, it was noted that the Department of Defense had identified several expanding threats that might challenge the current NC3 systems; in turn creating a need to procure new systems. The 2018 NPR indicates that China and Russia have developed capabilities that could potentially threaten space-based systems; in addition, the introduction of modern information technologies poses potential cyber vulnerability, which "has created new challenges and potential vulnerabilities for the NC3 system." Furthermore, many NC3 systems entered service in the 1970s. Many, like the Strategic Automated Command and Control System) are archaic, reaching the end of their life, or are no longer supported due to obsolete components. This makes maintenance impractical or extremely expensive. The NC3 architecture is composed of about 160 individual systems. At a high level, the NC3 architecture can be reviewed in two different categories, early detection and communication.[72] Finally, as our decision makers are faced with new complexities of multiple nuclear weapon armed adversaries a potential lack of experience and preparedness to respond to a first strike attack effectively could result in recommendations to the President made in haste. Artificial intelligence in this field and in the decision process could help or hurt within the deterrence calculus depending on how it is deployed.

Future Maximum Justification

(0.8) The ability to create secure and invulnerable network capabilities is key to ensuring NC3 capabilities remain robust to authorized command and control. This can be accomplished through technologies and systems such as intrinsic use control, developed at LLNL, where weapon arming functions are shielded from external signal interference and greatly decrease the chance for

---

[71] Nuclear Command, Control, and Communications (NC3) Modernization – Congressional Report written by Amy Woolf.

[72] The Congressional Research Service Report, dated December 8, 2020, refers to the 2018 NPR which will be updated in the next month or two. The document, while over a year old, still holds true. Dominant capabilities, which the United States has controlled for many years, are now being challenged.

unauthorized use[73]. Development of quantum signaling could also lead to rapid increases in NC3 capabilities, however, technologies such as this could also lead to increased decoherence that may be counterproductive to military strategies. Finally, a better balance of structure of the size and organization of executive command and control personnel groups that recommend when to launch nuclear weapons could decrease p(cost|~action). Artificial intelligence applied in the decision process might help with compressed timelines.

Trend

(0) Trend for NC3 deployability is flat given the current state of secure communications technology and upgrades that are being implemented through Department of Defense modernization programs. However, the robustness of command-and-control capabilities is showing signs of vulnerability and the general increase of network cyber-attacks (that are accelerating in rate and magnitude) have shown that additional attention to this hardware is required in the time-horizon of this assessment. This will help ensure that as modernization efforts are implemented, they are consistent with the security environment of the future.

SURVIVE FIRST-STRIKE

Current Justification

(0.7) NC3 capabilities are expected to survive 1st Strike with some existing limitations. According to Perkovich and Vaddi, NC3 may be vulnerable to long-range precision strike weapons or autonomous weapons systems.[74] However, the U.S. has a distributed command-and-control architecture that increases robustness with a relatively deep backup hardware infrastructure (to combat decapitating attacks). While this has been a concern for a very long time, only the increase in cyber activities seems to have changed. Without cyber threats this capacity would rank much higher due to the given distributed system and hardened facilities. Unfortunately, much of our system now relies on space assets to assist in surviving first strike attacks. Therefore, if many of our space assets are attacked, it may create a significant deficiency in command-and-control capabilities.

Future Minimum Justification

(0.4) The future minimum is based on the deprecation of our command-and-control architecture due to adversarial red increases in capabilities to block and deny U.S. NC3 capacity. While the hardware

---

[73] *See*: https://ipo.llnl.gov/index.php/technologies/software/intrinsic-use-control-cybersecurity-and-anti-counterfeiting-electronic
See Also: https://www.llnl.gov/news/lawrence-livermore-scientist-develops-uncrackable-code-nuclear-weapons

[74] Proportional Deterrence by Perkovich and Vaddi – with additional references: Sources: Hans M. Kristensen and Matt Korda, "United States Nuclear Forces, 2020," *Bulletin of the Atomic Scientists* 76, no. 1 (2020); Ronald O'Rourke, "Navy Columbia (SSBN-826) Class Ballistic Missile Submarine Program: Background and Issues for Congress," R41129, Congressional Research Service (updated October 7, 2020), https://fas.org/sgp/crs/weapons/R41129.pdf; Tyler Rogoway, "USAF's Controversial New Plan to Retire B-2 and B-1 Bombers Early Is a Good One," The Drive, February 12, 2018, https://www.thedrive.com/the-war-zone/18410/usafs-controversial-new-planto-retire-b-2-and-b-1-bombers-early-is-a-good-one; Amy F. Woolf, "U.S. Strategic Nuclear Forces: Background, Developments, and Issues," RL33640, Congressional Research Service (updated December 10, 2020), https:// crsreports.congress.gov/product/pdf/RL/RL33640/65; Kingston Reif, "U.S. Nuclear Modernization Programs," Arms Control Association, August 2018, https://www.armscontrol.org/factsheets/USNuclearModernization; Megan Eckstein, "Navy Beginning Tech Study to Extend Trident Nuclear Missile Into the 2080s," USNI News, November 14, 2019, https://news.usni.org/2019/11/14/navy-beginning-tech-study-to-extend-trident-nuclear-missile-into-the-2080s

architecture is distributed, it is not an overwhelming quantity of targets, therefore the system is expected to only partially survive and certain capabilities within the system are expected to be degraded.

Future Maximum Justification

(0.9) The U.S. is currently updating and modernizing the entire NC3 system. The effort, which started in 2019, is expected is expected to continue until 2028. While specifics for most of these efforts are tightly controlled or classified, it is expected that many of the upgrades will work to increase the robustness of command-and-control systems, including further distribution of architecture, continued hardness against vulnerabilities from cyber-attacks, and improvements in the ability to ensure the President is the sole authorizing authority over nuclear weapon use.

Trend

(0) Because capabilities are being enhanced, the trends for NC3 capabilities to survive first strikes are flat, but the modernization efforts are likely progressing at the same rate that the adversary is developing advanced cyber espionage capabilities. Increases in cyber-attack rates and magnitudes, however, can also be countered by ensuring that NC3 architecture is modernized in methods and functions that mitigate the severity of attacks. This can be accomplished through assurance that modern NC3 capabilities employ the latest cyber defense technologies and rely on capabilities such as intrinsic use control.

IMPOSE COST

Current Justification

(0.7) As stated earlier, the U.S. NC3 system includes space- and terrestrial-based platforms, as well as computer architecture and other hardware that enables these platforms within the current command-and-control infrastructure. Some weaknesses exist, and adversaries are expected to target U.S. NC3 systems, but modernization efforts are being taken very seriously and advances are expected to address weaknesses. This will enable delivery systems and nuclear weapons to be launched as ordered.

Future Minimum Justification

(0.5) The future minimum depends upon consistent funding for the modernization of the NC3 system. If no upgrades or modernization occurs, then the system would be very vulnerable to cyber-attacks and other emerging technologies. If the system were in fact disabled, then the communication to request launch could be delayed or parts of the NC3 system may not receive the message to launch and impose cost. But once the command is given there is high confidence that retaliation will be carried out and the cost will be imposed, even if there are some degraded capabilities and a full retaliation launch command cannot be given.

Future Maximum Justification

(1) As new threats are prompting the government to invest heavily in modernization efforts of the NC3 system, the deficiencies in cyber vulnerabilities will be overcome. This is expected to ensure a system that is resilient against attacks and enabling of imposing cost on the adversary.

Trend

(1) Nuclear Command, Control, and Communications is a paramount capability to assure that nuclear weapons are utilized only when authorized by the President and against adversaries in conflicts that are

proportional for their use. Because the current system is highly distributed and there are robust modernization efforts underway, we judge the NC3 trends to be increasing.

Sensors

DEPLOYED CAPABILITY

Current Justification

(0.9) The U.S. maintains a distributed ballistic missile early warning system (BMEWS) of radar stations[75] as well as well as a space-based infrared system (SIBRS) of satellites[76]. Both of which can provide early warning and attribution of any conceivable massive nuclear first strike. Additionally, the Integrated Undersea Surveillance System (IUSS) provides timely reporting of potentially strategic submarine activity[77]. Within this system, our detection capabilities (including radars, satellites, and processing systems) provide "unambiguous, reliable, accurate, timely, survivable, and enduring"[78]. Thus, it seems inconceivable that our adversaries would perceive that they could launch a massive first-strike on the U.S. without it detection that an attack was occurring and appropriately attribute the attack to the responsible adversary. Thus, we assess that our adversaries will view our deployed sensor capability as playing its role to maintain high probability that if they launch a massive nuclear first-strike on the U.S. we will be able to respond with a nuclear second-strike (i.e., the $p(\text{U.S. nuclear weapon 2nd strike}|\text{red nuclear weapon 1st strike})$ term in deterrence calculus will be large). There is the concern of false detections in the sensors that might trigger the U.S. to falsely believe that there is a first-strike occurring, which works to increase our adversary's perceived probability of us imposing a cost even if they do not launch a first-strike (i.e., increase $p(\text{U.S. nuclear weapon 2nd strike}|{\sim}\text{red nuclear weapon 1st strike})$ in the deterrence calculus) and decrease effectiveness of our deterrent. However, given the redundant and dispersed sensors (radar, satellites, etc.) the likelihood for false detections that cannot be ruled out by another sensor set is low.

Sensors Assessment Summary	
Current	The current sensor network is sufficient to credibly detect, attribute and provide necessary targeting information.
Future Minimum	Adversaries are developing anti-sensor weapons; however, these are unlikely to affect the base secure second-strike mission significantly.
Future Maximum	There are plans and funding to develop even more extensive sensor networks as well as data processing methods to make this subcomponent even more credible.
Trend	The trend is steady as enhanced capability is largely countered by adversaries placing the sensor network more at risk.

Furthermore, the U.S. deterrent also relies on sensors to provide feedback of key attributes of warhead systems and platforms. These sensors can provide advanced knowledge of weapon functionality to ensure weapons are operations as well as when weapons are vulnerable to adversarial strike in close-quarters and strategic combat. These sensors increase the adversary's perception of the U.S. for credibly fielding a secure retaliatory strike.

---

[75] U.S. Space Force, "Upgraded Early warning Radars", U.S. Space Force Fact Sheets, March 22, 2017, https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197738/upgraded-early-warning-radars/

[76] U.S. Space Force, "Space Based Infrared System", U.S. Space Force Fact Sheets, March 22, 2017, https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197746/space-based-infrared-system/

[77] Commander, Undersea Surveillance, "About IUSS", accessed 2022-01-13, https://www.csp.navy.mil/cus/About-IUSS/

[78] Defense Primer: Command and Control of Nuclear Forces – Written by Amy Woolf, Specialist in Nuclear Weapons Policy – CRS-IF10521 (11/19/21)

Thus we assess that the current deployed sensor capability contributes to a credible deterrent.

Future Minimum Justification

(0.6) When considering how science and technology might impact the sensor sub-component's contribution to the second-strike deterrent of a massive first strike, it is important to realize that the sensor related mission requirements are a relatively low bar, due to the fact that we rely primarily on sensors to inform when nuclear first strikes are occurring or when weapon systems are not functional. Thus, even though adversaries continue to develop new anti-satellite (ASAT) capabilities[79] threatening SIBRS as well as hypersonic weapons[80] that may eventually threaten BMEWS, the increased proliferation of sensors and possibility that if the U.S. strategic early warning system is targeted by an adversary in a widespread attack that it will be treated as a sign of a precursor to a first-strike strike means that this probability is likely to remain high. Perhaps the greatest science and technology threat for the sensor sub-component negatively impacting is a coordinated cyber-attack taking down the entire sensor network or injecting a false first-strike signal. The possibility could greatly increase $p(\text{U.S. nuclear weapon 2nd strike} | {\sim}\text{red nuclear weapon 1st strike})$ and degrade our overall deterrent, however, it is unlikely that an adversary would intentionally credit themselves to an attack that was not realized. That said, as long as the U.S. maintains secure sea- or air-legs of the triad it will reduce the need to respond immediately to the false signal and dampen this effect. Somewhat related is the threat to parts in the sensor supply chain. While hypersonics may be seen as a potential spoiler since they are capable of striking the U.S. homeland from the south where our sensor network is weakest, it is unlikely that they would be able to develop a massive first strike hypersonic force before we could respond with new sensors capable of achieving the detection and attribution component of the mission.

Future Maximum Justification

(1.0) DoD officials have argued that future conflicts may require decisions to be made within hours, minutes, or potentially seconds compared with the current multiday process to analyze the operating environment and issue commands. They have also stated that the department's existing command and control architecture is insufficient to meet the demands of the NDS. DoD proposes the Joint All-Domain Command and Control (JADC2) concept as a method to counter potential adversaries' ability to disrupt U.S. forces' combat operations. The JADC2 concept envisions connecting sensors from all of the military services—Air Force, Army, Marine Corps, Navy, and Space Force—into a single network, thus eliminating the possibility that an adversary could cripple a U.S. force by taking out a single, key sensor. JADC2 is intended to enable commanders to make better decisions by collecting data from numerous sensors, processing the data using artificial intelligence algorithms to identify targets, then recommending the optimal weapons—both kinetic and nonkinetic (e.g., cyber or electronic weapons)—to engage the target.

---

[79] Jeff Foust, "Russia destroys satellite in ASAT test", Space News, November 15, 2021 https://spacenews.com/russia-destroys-satellite-in-asat-test/; Jeff Foust, "India tests anti-satellite weapon", Space News, March 27, 2019, https://spacenews.com/india-tests-anti-satellite-weapon/

[80] Chandelis Duster "Top military leader says China's hypersonic missile test 'went around the world'" , CNN, November 18, 2021, https://www.cnn.com/2021/11/17/politics/john-hyten-china-hypersonic-weapons-test/index.html

The U.S. is increasing its investment in ballistic missile warning systems, such as the next generation Overhead Persistent Infrared (OPIR) ballistic missile warning system[81]. Additional research investments also include a focus on the sensor sub-component addressing the growing hypersonic threat[82]. There is the potential with artificial intelligence (AI) and quantum computing (to break encryption) that we could have significant indication and warning (I&W) of a massive first strike before it is launched by our adversary. The capability of the U.S. sensor hardware is already high but these investments could increase its delivered capability higher.

Furthermore, as sensor capabilities are increased and integrated into future weapon systems, it is possible that these sensors can enable U.S. weapon systems to potentially avoid first strikes by autonomously maneuvering the system from the adversarial damage impact-point.

Trend

(0) Despite the large investments in the sensors delivered capability we asses that their contribution to the second-strike deterrent will remain steady primarily because they are already quite capable. These investments will also largely balance adversary investments in ASATs and hypersonics. Two caveats are that if our adversaries think that we will rely on AI for left of launch alert, or if our adversaries develop across the board false flag capabilities. Then this this may greatly increase their $p(\text{U.S. nuclear weapon 2nd strike} | {\sim}\text{red nuclear weapon 1st strike})$, and degrade the fielded deterrent capability.

However, the ability for our sensors to also inform the weapon systems and strike environments enables a robust deterrent that ensures capable weapon systems are deployed and that delivery platforms can impose cost when needed.

SURVIVE FIRST-STRIKE

Current Justification

(0.7) As previously noted, current sensor technology is adequate to define when probable ballistic missile launch occurs and the originating location of launch. Thus, while U.S. sensor hardware may be vulnerable, they can achieve the necessary mission before they are potentially destroyed. It is possible that a counter-force targeting strategy might be impacted by the weakness of sensor hardware to survive a coordinated attack. The U.S. would still have a viable counter-value strategy capability, however if the adversary only launched a counter-force attack on the U.S. it is not clear that it would be wise to launch a counter-value second-strike and risk further retaliation with a counter-value third-strike on the U.S.

---

[81] "The Space Force requested $2.3 billion in FY2021 RDT&E funding for the development of a next-generation Overhead Persistent Infrared (OPIR) ballistic missile warning system. This amount represents nearly an $800 million increase above FY2020 appropriations. The FY2021 request intends to develop the next generation of survivable space-based missile warning OPIR platforms. The Space Force contends that this program will deliver improved missile warning capabilities that are more survivable against emerging Chinese and Russian threats.", Congressional Research Service, *Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition*, June 4, 2020, p.20

[82] Sandra Erwin, "DoD agencies to invest more than $1 billion in low-Earth orbit space technologies", *Space News*, May 30, 2021, https://spacenews.com/dod-agencies-to-invest-more-than-1-billion-in-low-earth-orbit-space-technology/

Future Minimum Justification

(0.5) Space has recently been designated a warfighting domain[83] and as such it is expected that U.S. space-based ballistic missile warning satellites will become more vulnerable as actors continue to develop ASAT capabilities. Additionally, hypersonics could increase the threat against ground-based radar systems. S&T developed by the commercial industry is not likely to detrimentally affect capability beyond enhancing some adversary's technical readiness level, but commercially available targeting leveraged by some of our adversaries may increase their overall effectiveness. All said, it is not foreseeable that U.S. sensors will not survive long enough to ensure their ability to credibly conduct a secure second strike.

Future Maximum Justification

(0.9) Increased numbers, capabilities, and distribution of sensor hardware offer the promise of enabling the U.S. sensor network to survive a first strike. Additionally rapid launch technologies can help replace lost sensors and maintain all nuclear response strategies available to the President (we might not be able to stop a fait acompli, but we could potentially prevent more extensive coercion and attacks). Furthermore, development by the U.S. can facilitate enhanced survivability through detection and early warning or identification of where/when adversary forces are within strike postures, hence enabling an appropriate state of readiness of U.S. strategic forces at time of 1st Strike. Future weapon systems may have capability to incorporate avoidance technology that enables sensor and weapon systems to relocate/translocate to avoid first strike without full launch (i.e., striking to impose cost). Commercial technologies are likely to be leveraged regardless of U.S. technology readiness level (TRL), therefore capability using early warning/detection can be co-opted for increased capability.

Trend

(1) While the U.S. sensor network will remain vulnerable to enemy attack the anticipated ability of the U.S. to leverage commercial S&T in addition to S&T developed through increased DoD investment will largely balance and exceed adversary counter-capability. Especially coupled with the relatively low bar set for the sensor hardware.

IMPOSE COST

Current Justification

(0.8) As described by the context and discussions above, the sensors involved in actually imposing a cost in response to a massive first strike with U.S. nuclear weapons are relatively basic and robust once the U.S. has decided to launch a retaliatory strike. While accuracy dependent sensors (e.g., GPS and onboard tracking systems) are required to ensure minimal collateral damage, these capabilities are well proven for launching a retaliatory strike to a massive first-strike on the U.S. homeland. For such retaliation, approximate ballistic trajectories can also suffice for imposing a proportional cost on the adversary.

Future Minimum Justification

(0.6) If adopting a counter-force strategy, and the adversary successfully takes out most of the sensor network then it will negatively impact the U.S. ability to respond to a counter-force first strike with a counter-force second strike. That said the bulk of the mission is based on the ability to credibly threaten a large response cost on the adversary. This should remain possible even if targeting related sensor are

---

[83] Benjamin Bahney and Jonathan Pearl, "Why Creating a Space Force Changes Nothing", Foreign Affairs, March 26, 2019.

lost during the first-strike attack. The ability for adversaries to develop S&T that can mask targets by creating false cyber-based diversions is extremely unlikely, but not impossible and likely to increase at the far-end of this assessment horizon. The ability for adversaries to obscure GPS capabilities/tracking systems that U.S. weapon systems rely upon is more likely but requires specific targeting of satellite systems that takes away from strategic targets within the U.S. Commercial S&T is unlikely to destabilize GPS and tracking systems in terms of target launch capabilities, but commercial S&T may be developed that can obscure or mask targets from onboard systems through new material technologies and coatings.

Future Maximum Justification

(0.9) As sensor technologies improve and sensor networks becomes more robust, it is possible that the U.S. can more accurately target and impose cost proportionate to the first strike, as well as hold targets at-risk from longer ranges. Improvements and development of redundancy in GPS and tracking systems is unlikely to provide much additional benefit. Commercial S&T is likely to be co-opted and leveraged regardless of U.S. TRL for unique technologies.

Trend

(0) It seems like there will continue to be a balance between sensor number and capability with adversary's ability to destroy blue sensors (U.S. sensors are growing more capable while they grow more vulnerable). We also expect a flat trend due to trade-offs between anticipated adversary TRL being low and commercial S&T being the major disruptive/destabilizing factor. This trend is dependent upon the ability of U.S. to continue leveraging commercial technologies in general.

Case Study Conclusions

Within this case study, we have assessed the Secure 2nd Strike capability to deter a massive nuclear first strike using a new tool that informs the likelihood of success of deterrence based on the deterrence calculus. This assessment informs the key capability of the U.S. strategic deterrent upon which the U.S. bases its national security and national sovereignty. As assessed, we are confident that the Secure 2nd Strike is technically capable and proportional to deter the actions of an aggressor that can launch a massive nuclear 1st strike. To enable the assessment of the tool as a deterrent capability, we have further developed the mission "kill-chain" requirements and design of the Secure 2nd Strike capability for a focused assessment of the capability. Through this tool we have provided a science and technology focused detailed assessment of the design components and hardware that thereby allowing us to assess the current state of the component as well as potential future S&T enhancements or degradations that affect each of the components with respect to support of the detailed mission "kill-chain" requirements. Finally, we have trended these S&T enhancements and degradations to provide insights for support of the deterrence calculus over the next approximately 10-years.

Warhead Assessment Conclusions

The development, stewardship, and certification of nuclear warheads is a key responsibility for NNSA laboratories, including Lawrence Livermore National Laboratory. The nuclear warhead arsenal within the United States is extremely robust to meets current and future deterrence needs, however, there is also significant space for improvement to support the U.S. deterrence policy and mission. Three key finding for improvements in the nuclear stockpile that reduce production cost and enable broadened applicability to the deterrence calculus are: 1) incorporate "modularity" within nuclear warhead design to enable broad implementation across a variety of delivery systems to hold as many potential targets at-risk; 2) ensure functional warhead lifecycles are rational and both enable and permit warhead development and fielding strategies with tractable engineering and production solution; and 3) engage in warhead modernization programs that both incorporate new science and technology that can mitigate known deficiencies and also enhance component knowledge that enables warheads to meet or exceed the stockpile to target sequence environments. To meet these challenges, several specific lines of effort can be pursued.

First, clear delivery vehicle boundary interfaces can be established that will provide robust mechanical and electrical envelopes for warhead design. Within this design space, a multitude of new or unique designs can be matured independent of delivery vehicle lead-ties that enable changes to the nuclear and weapon effects coupled to the target without requiring changes to the delivery vehicles. Nuclear effects influences could include warheads with enhanced radiation outputs, decreased blast effects, or other unique coupling-mechanisms. The ability to field new designs, independent of delivery platform, will significantly enhance the ability for the U.S. to impose nuclear retaliation costs without significant destabilization of other factors within the deterrence calculus.

With current stockpile warhead design lifespans approaching 40 years in the field, a number of previously novel innovations have now become dated or deprecated. The ability to maintain designs and assets beyond their originally designed lifespan is extremely difficult and resource intensive. Therefore, development of individual warhead lifespans that are limited to 10-20 years, for example, can be supported by robust S&T programs that can study and assess known weapon responses to defined environments with extremely high confidence without the intensive resources required to maintain systems and assets indefinitely. Furthermore, modern production capabilities would also benefit from this shortened lifespan by mitigating factory limited life component exchanges and other costly maintenance programs that are required to assure working components with deprecated technology. The modern production capabilities also require, and are predicated on, the ability to maintain a consistent quality supply chain for raw materials and goods. New material fabrication methods as well as advanced assembly techniques are likely to be inspired by commercial S&T programs and will provide excellent cooperative venues that will help assure products meet their design specifications. The ability to limit warhead lifecycle spans to this time-scale does not imply that after 10-20 years, warheads need to be re-designed, it implies they only need to be replaced with like-for-like capabilities as determined by the security environment.

Finally, warhead modernization programs must base efforts in the ability to incorporate modern technology and capabilities within each update, not simply to refresh materials. Utilization of test capabilities for modern-era investigations will facilitate U.S. understanding of component interactions and hardware operational envelopes. Test facilities designed to mimic intense A2AD environments (blast, thermal, fragment, etc.) that are dedicated to assurance and certification of nuclear warheads will quickly provide dividends to material and hardware studies as part of the stockpile stewardship program.

Delivery Vehicle Conclusions

Ground-Launched Systems

The current U.S. ground-based nuclear ICBM deployed capability is sufficient to ensure a Secure 2nd Strike capability is technically credible. Despite their vulnerability, due to being fixed targets, missile launch can be rapidly executed with delay limited only to the checks and balances for authorized nuclear use, regardless of time or target. The current U.S. ICBM force is well dispersed within the geographic locality. Modernization programs are currently underway and expected within the next decade. While the U.S. may not have enough ICBMs to fully absorb a first-strike, there are sufficient numbers such that the adversary must commit a large number of their force to destroy them, which produces high signal-to-noise ratio of their intentions and limits targeting of air or sea-based nuclear forces. Additionally, given the fact that the ICBM force is located on the continental U.S., any debilitating attack on the ICBM force would likely increase the probably of the U.S. responding with a strong second-strike.

The primary reason we don't assess this capability higher is that the ICBM vulnerability means that the U.S. must use them quickly in the event of a massive first-strike, which in turn increases the adversaries perception that the U.S. might intentionally or inadvertently launch a nuclear strike against an adversary, even if they don't actually launch a first-strike (i.e., $p(\text{U.S. nuclear weapon 2nd strike}|{\sim}\text{red nuclear weapon 1st strike})$ is non-negligible) leading to instability and decreasing our deterrent effect. The increasing pace of potential conflicts and increase in the size of adversary arsenals will likely execrate the factor and further reduce the credibility of the land-based deterrent.

Sea Systems

Naval nuclear submarine assets (SSBNs) have the ability to move nearly unimpeded throughout the world's oceans and Areas of Responsibility (AOR). This is largely due to the inability to track or exclude SSBNs through sensors or diagnostics. SSBNs also have the ability to rapidly strike nearly any target from a range that is close enough to mitigate most chances of early detection. Three key findings from the assessment of the sea-based delivery vehicles are: 1) Undetectable freedom of movement must be maintained which includes mitigating potential vulnerability to exploited commercial S&T sonar or scientific animal or commercial-resource tracking networks; 2) system modernization programs must maintain political continuity due to the extensive lead-time for product realization; and 3) the advancement of capabilities through automation and remote designs can provide force multiplication in multi-polar security environments dominated by great power competition.

Detection and tracking of SSBNs in open water AORs remain one of the most difficult S&T challenges within the deterrence capability. While the specific quantity of SSBNs is small, their freedom of operations enables a robust, and quite possibly the most significant asset within the Secure 2nd Strike capability. Explicit detection methods by adversaries appears to be far from realization, however, the increased interest in open ocean and sub-surface sea-based resources for commercial gain has enabled commercial S&T efforts to determine where these resources can be gained from, extracted, and then processed. To aid this commercial effort, networks of research tracking and detection systems are likely under development and may present vulnerabilities that could be exploited in the future and be utilized to track submarine nuclear forces.

Development and fielding programs for modernization have an incredibly long lead time and are worth billions of dollars in commercial interests. Commercial S&T efforts that can facilitate enhanced and expedient material fabrication could potentially decrease modernization programs by cutting lead times for procurement from nearly two-decades to single-administration spans of effort and would mitigate years of effort from capital resources, enable superior quantities of deployed assets, and significantly increase the favorable deterrence calculus. However, gains made within the deterrence calculus for costs imposed may be offset by significant decreases in the benefits gained by adversarial inaction resulting in null-changes to the overall calculus assertion.

Finally, advancements in the ability to field autonomous and drone-based underwater nuclear strike packages is one venue for S&T to significantly shift balancing strategies. The use of smaller autonomous capabilities can enhance the SSBN capabilities by eliminating the potential for human error or irrational actions that could lead to detection. However, as with capabilities to field products more rapidly, the use of underwater drone technologies could also offset the deterrence calculus and may increase the potential for arms races.

Air-Delivered Systems

U.S. air delivery systems include long range bombers and fighter planes. The B-52H has been a workhorse for this capability since the early 1960s and is expected to stay the course into the 2050s, it will continue to be the delivery vehicle for the modern air-delivered systems. The B-2 Spirit is stealthy but expensive, and is expected to remain in operations into the mid-2030s, however, the new stealth capable B-21 Raider is expected to fulfil multiple needs for future of the U.S. air-delivery systems. The B-21 is being designed to be functionally capable of inflicting nuclear costs as well as conventional costs. The bomber was the key to success during the cold war and the latest advancements in stealth technology will ensure its place as a strong deterrent in the future. One observed challenge is where to stage the bombers as many of the SAC bases were closed after the cold war was considered over. Reopening some of these bases or having current bases serve as multiple fighter/bomber wings should be considered as a hedge against the long traverse-to-targets that is experienced by the current bomber force.

Nuclear Command, Control, and Communications (NC3) System Conclusions

The mission of the NC3 system is to ensure control over all nuclear forces and strategic operations. In order to carry out this mission, the technology must be able to provide timely warning of an imminent attack, supply situational awareness to the various commands and assure effective and secure communications between the national command authority and the commander-in chief. This system could be considered the brain of the deterrent, ensuring all communication and delivery information for our nuclear arsenal. The current NC3 system is in the process of modernization to replace and upgrade many of the components that are vulnerable, no longer supported and antiquated. Many of NC3s vulnerabilities are emerging concerns. The system must be secure and resilient and impervious to large vulnerabilities. The timeline for modernization extends for the next many years (2019 – 2028) and that time will pass by quickly. “The Pentagon has recently recognized the urgency of building a resilient and adaptable NC3 system and has put USSTRATCOM in the lead of the NC3 modernization program. USSTRATCOM is well positioned to determine the best course of action for NC3 modernization within the broader context of U.S. nuclear modernization and changes to posture and policy.”[84] Improvement of these systems, ensuring security, resilience, and functionality, is paramount and must be achieved, lest the body of the nuclear deterrent be informed.

Sensor System Conclusions

The three primary roles sensors play in affecting the deterrence calculus related to deterring a 1st strike on the U.S. with a secure nuclear weapons second-strike tool are: detecting a first-strike attack on the

[84] Perkovich and Vaddi, Proportionate Deterrence

U.S., attributing that attack to the responsible adversary, and providing the information necessary to target the adversary assists with our nuclear second-strike force. These roles are a relatively low bar for the current U.S. satellite, radar, and sea-based sensor networks. While sensor networks are currently vulnerable to adversary attacks (and will become more vulnerable increased adversary investment in ASAT, hypersonics, and cyber related adversarial tools) they are able to achieve their mission before being destroyed. Thus, the current sensor network contributes to a credible deterrent and is expected to do so for at least the next ten-years.

Sensors will also play a greater role in assurance that U.S. weapon systems will be ready and prepared to respond in a Secure 2nd Strike. The ability for sensors to identify if a particular weapon system is online and functional is a major factor to impose costs against an adversarial massive first strike. Furthermore, the ability for future sensors to autonomously translocate or relocate assets during a first strike will enable a stronger retaliatory strikes. During adversarial A2AD confrontation, sensors can also facilitate mitigation of damage to delivery platforms by enabling close-quarter maneuverability and avoidance of A2AD systems.

Perhaps the greatest threat to the sensor hardware is a false-flag cyber-attack that could manipulate the U.S. into decisions against a nation that were not instigated. Although this would need to be broad and comprehensive offensive against the U.S. given the distributed and redundant U.S. sensor network. Potentially the greatest potential for enhancing the sensor sub-component is with artificial intelligence (AI) and quantum computing (to break encryption) that we could have significant indication and warning (I&W) of a massive first strike before it is launched by our adversary (i.e., left-of-launch warning).

Discussion and Implications for Lawrence Livermore National Laboratory and United States Deterrence Policy

Through this report, we have provided a methodology and tool-kit for the development of capabilities, or tools, that will enable the assessment of specific deterrence capabilities to support a robust national defense strategy for the current strategic security environment. By matching threat actions to deterrence tools, future analysts can apply this methodology to assess the efficacy and proportionality of technical deterrence solutions relative to the threat actions to maximize and enhance the U.S. strategic deterrence capabilities. Furthermore, this tool-kit enables analysts to perceive insight into gaps within existing or postulated strategic deterrence capabilities. These insights can be used to trend ongoing research and development programs for comparison to the future effectiveness of a specific deterrence capability. By understanding the full scope of a deterrence tool, including both abilities and limitations, U.S. research laboratories, such as Lawrence Livermore National Laboratory, can effectively propose, develop, and prototype future deterrence capabilities to meet national security needs.

As we have shown in this report, to meet the challenges of a modern integrated deterrence, existing deterrence tools can be compared with conceptual tools that enhance United States deterrence capabilities against a range of aggressive actions or are tailored to a single unique aggressor action. Conceptual new tools can begin the design path informed by the concept of operations (e.g., adversarial actions) that the tool will presume to effectively deter and employ a framework for success established by deterrence mission requirements that represent the full mission profile of the tool, described in this report as the “Mission Kill Chain.” With mission requirements established, analysts can evaluate a specific tool to determine the suite of hardware that is required to fulfill the mission profile, including hardware such as detectors for action initiation, communications, delivery platforms, and cost imposition systems. Hardware products that can be developed or implemented as a deployable capability are then assessed in detail for technical capability to meet the mission requirements as well as for proportionality with respect to the deterrence calculus. The completed assessment is then re-evaluated for application through the deterrence calculus to the action it is intended to deter, therefore iterating the entire deterrence analysis cycle.

With respect to technical capability assessments, aspects such as reliability, survivability, and damage effectiveness can be analyzed completely. Detailed technical assessments also support analysis of research and development (R&D) trends and future effectiveness given the arbitrary perspectives of holding current R&D levels steady, increasing blue R&D levels, or increasing red R&D levels. The detailedness of the analysis enables high confidence in capability planning, fielding, and modernization timelines with respect to the evolving nature of technology. Proportionality analysis provides a rigorous review of indeterminate variables, such as the relationships of cost of targets to adversarial value, trade-space in benefits as they influence the deterrence calculus, and potential negative connotations for the deterrence calculus variables.

To support the development of this methodology, we have provided a high-level, yet informed assessment of the U.S. nuclear deterrence capabilities within this report. However, there are many subtle nuances that must be explored further in follow on analysis and assessments. In this report, we have combined both technical capability and proportionality assessments into a single seamless assessment in the interest of resource availability, however, future application of the deterrence assessment matrix and application of this methodology fully supports and allows these assessments to be conducted independently with appropriate iterations. Additionally, this methodology and the assessment herein are conducted using fully unclassified information from academic and open sources such as the Congressional Research System. Future assessments should be conducted using as accurate and complete knowledge as possible.

We find that while the U.S. nuclear deterrent is technically capable of deterring a broad range of actions, it is limited by the principle of proportionality coupled with a perceived cost of nuclear weapons. Meaning that nuclear weapons are typically only good at deterring other nuclear weapon attacks or intentional and costly non-nuclear actions that threaten the primacy of the United States within the global order. Changing the perception of the proportionality of nuclear weapon use will require significant efforts to change the effectiveness of against tactical and strategic warfare threats against actions other than those involving nuclear weapons. This could be accomplished through new design proposals and certifications of weapon outputs to specific destructive effects.

From our detailed science and technology focused assessment of the U.S. nuclear strategic arsenal to deter a massive nuclear first-strike on the U.S. homeland we find that delivery vehicles followed by nuclear command, control, and communications (NC3) are the sub-components at the highest risk of being disrupted by future science and technology developments. This is primarily driven by sensor, artificial intelligence, and cyber related technologies. Intelligence, surveillance & reconnaissance related technologies offer the most potential for enhancing our nuclear deterrent in the future. However, there is significant room for improvements within the warheads category. Current warhead designs are generally dated and were purposefully designed during the Cold War era. Warhead modernization efforts have enhanced some aspects of target envelopes. However, many additional warhead improvements could be realized by creating common interfaces with delivery vehicles that allow for block-upgrade modularity with more independence of the delivery platform, enhancements in lifecycle management that reduce dependency on rare or invaluable materials by allowing designers to focus on shorter lifecycle design principles and enhancing knowledge of common material interactions, and sub-system testing of warhead safety and reliability environmental envelopes.

In general, technological solutions are a necessary but double-edged sword, with frequent correlation between countervailing levers within the deterrence calculus. For example, increasing the technical ability to deter an adversary's action through threat of cost imposition often increases the adversary's perceived need to act hostilely for fear of having a cost imposed on them if they don't act, potentially creating a net negative deterrent effect[85]. In part this can and should be managed by the purveyors of technological solutions, however, it is necessary to couple technical solutions with political solutions. Since much of the U.S. deterrent credibility is limited by the principle of proportionality, and not technical capability, it would be in the best interest of the country to consider technical solutions in the context of the principle of proportionality as well as their technical capability.

It is our recommendation for LLNL, as the primary sponsor for the body of work contained within this report, that efforts to revisit certain detailed assessment areas should be distributed within the laboratory organizational structure for follow on analysis of nuclear deterrence capabilities. Numerous organizations that support stockpile stewardship have the necessary skill and capabilities, developed through the robust stockpile stewardship program, and can lead efforts for development and resolution of the science and technology challenges developed and identified within this report. As with any challenge, trade-space for effective deterrence solutions must be balanced between the technical capabilities and the principle of proportionality.

Deterrence is ultimately an operation in the cognitive domain, LLNL would benefit from coupling the extensive subject matter expertise in this area with its existing technical weapons design capability to expand and enhance America's deterrence portfolio. LLNL has already taken important initial steps in this direction by trying to understand how our adversaries perceive our deterrent tools through the activities of the Center for Global Security Research. That said, understanding how our adversaries perceive the cost imposed by an array of U.S. deterrent tools could help us better design an integrated deterrent.

Of similar importance is the need to better understand and manipulate the general perceived cost of a given deterrent tools' actions[86]. As we discussed at length, nuclear weapons have an inflated perceived cost which significantly limits its broader utility as a deterrent tool relative to the technical capability. By bringing the inflated perceived cost more in-line with the actual cost their applicability to other deterrence missions could be expanded. This could be done with a strategy of slowly providing observations or data of the actual cost of nuclear weapons to the general populations starting at the low-cost end[87]. However, the U.S. as a conventional superior power by most measures benefits

---

[85] See also the related discussion in Schelling, "Strategy of Conflict", pp230-231.

[86] Similar to jockeying to establish preferred limits (Schelling, Strategy of Conflict, p.262).

[87] Active testing is a way to start, followed by low-yield use against an isolated military target, etc., slowly increasing the actual cost and allowing enough time between uses and escalation for the uncertainty around the perceived cost to decrease at each step. It is not clear that you can 'pause' long enough between each time step

asymmetrically from the inflated perceived cost of nuclear weapons and should actively seek to maintain the inflated perception. Relatedly U.S. technical authorities and policy advocates should also consider the trade-space for developing or normalizing smaller 'tactical' nuclear weapons that may encourage less capable nation-states of pursuing limited nuclear warfare capabilities[88]. Similar perceived cost considerations should be given to all of the U.S. deterrent tools as well as adversary actions.

Within the context of nuclear deterrence at-large, this report has not assessed defensive or mutual-conventional capabilities to any substantive extent. To enhance a nuclear deterrence capability, one can certainly consider an alternative to lowering acceptance of escalation to nuclear weapons use by considering a deterrence by denial strategy, thereby encouraging adversaries to achieve their ends through more conventional means. This can be accomplished by increasing the A2AD capabilities of the U.S. and its allies, thus encouraging adversaries to commit a larger conventional force to overcome the A2AD. The increased conventional action an adversary would make enables a more proportional threat of a nuclear weapon retaliation.

We have noted the principle of proportionality has implications for any integrated deterrence strategy. Because there is no universal equivalency that relates the cost imposed in one domain to that in another domain, or against one target to that in another, it is difficult to determine what cross-domain or cross-target deterrence threats are perceived as proportional or credible. Similarly, the deterrer is challenged with making threats that they must be prepared to follow through on, and if they do not manage the perceived proportionality of their response, they risk balancing from political, economic, and social forces, both domestically and internationally. Thus, individual states may feel that there is more risk associated with some integrated deterrent strategies than with others when compared within the global order.

We have discussed how the various levers of deterrence within the deterrence calculus are often coupled for a unique deterrence tool. For example, improving a tools' capability to deny benefits is often coupled with its ability to punish, irrespective of the adversary's action or non-action, because the tool technical capability should be considered separately from the tool's implementation when accounted for in the deterrence calculus. Technological enhancement considerations for deterrence tools should consider the full deterrence calculus implications. Although not discussed in this report, we consider the deterrence calculus to be dynamic and thus users and analysts must also consider the continuous action-response chain implications where changes in one variable may fluctuate based on feedback from other variable changes.

The systematic approach to the development of requirements and assessment methods as we have provided in this report is key to building consistency in complex deterrence assessments. This approach enables critical review of current deterrence tools and strategies as well as determination of actions that

---

for observations to translate into decreased uncertainty before others react in proportion to the originally inflated perceived cost.

[88] Given our belief that the perceived cost curve of nuclear weapons rise rapidly for the general population, the lack of low-yield nuclear weapons does not significantly degrade our nuclear weapon deterrent . People understand the distinction between 'no nuclear weapons' and 'some nuclear weapons. They do not typically understand the distinction between 0.5kT vs 100kT. Thus if an opponent attacks with a low-yield nuclear weapon it should still be credible according to the principle of proportionality that we might respond with a 100kT nuclear weapon.

we aspire to deter. Detailed assessments of technical capabilities that support deterrence and the proportionality of a deterrence capability application to the cost imposed is imperative to assuring successful deterrence. It is our hope that by developing a prescriptive assessment methodology we can avoid deterrence missteps in the future[89].

[89] Much in the same way that the scientific method is obvious, its framework and the practice of it has enabled efficient advancement throughout numerous technical disciplines, often exponentially when correlated to the advancements achieved in certain fields.