EXPLORING THE REQUIREMENTS OF INTEGRATED STRATEGIC DETERRENCE

Workshop Report

August 2017

Center for the Study of Weapons of Mass Destruction / National Defense University
Center for Global Security Research / Lawrence Livermore National Laboratory

LLNL-MI-737637

Exploring the Requirements of Integrated Strategic Deterrence

A Workshop Jointly Convened by
Lawrence Livermore National Laboratory and National Defense University
11-12 July 2017

The workshop sought to gain a deeper understanding of how a more integrated approach to capabilities, operational concepts and plans could deliver a stronger deterrence posture to meet the challenges posed by advanced nuclear-armed adversaries in future regional crisis and conflict. More than forty subject matter experts gathered to discuss various aspects of integration and the ways in which U.S. strategy, policy and forces could adapt to enable more integrated approaches.

The workshop was organized jointly by the Center for the Study of Weapons of Mass Destruction (CSWMD) and the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory, and hosted by CSWMD. This report was prepared by Paul Bernstein (CSWMD) and Brad Roberts (CGSR). The views expressed here are those of the authors and are not an official policy or position of the U.S. Government.

What do we mean by integration and integrated deterrence?

For the purposes of the workshop and motivating the analytic thinking required to advance our understanding of this challenge, integration generally refers to leveraging the synergies among the various elements of the deterrence toolkit to create stronger or more decisive effects than otherwise could be achieved. A more expansive working definition might read as follows:

> *An understanding of the relationships among different types of capability at the strategic and operational levels and how they can be leveraged to achieve objectives for crisis management (pre-conflict deterrence), intra-war deterrence, and the management of escalation risk. The ability, enabled by this understanding and expressed in plans, to execute actions that optimally apply some or all of these capability types in support of these objectives.*

This can serve usefully as a working definition, and the workshop sought to advance a common conception along these lines. Under this broad definition, several distinct contexts for integration also exist. The program was organized to explore the question of what improved integration should mean in practical terms in these contexts, which include: offense and defense; nuclear and conventional; U.S. and allied strategies and capabilities; and covert and overt capabilities – with cyberspace and outer space as cross-cutting factors. At the same time, the workshop revealed that integration and integrated deterrence can be conceived in different terms. For example, a number of participants viewed integrated strategic deterrence as a frame for more systematic pursuit of deterrence in the “gray zone” or the lower end of the conflict spectrum. This is not surprising in light of real world events. Adversaries are prosecuting gray zone conflicts through strategies and operations that weave together soft and hard power instruments to achieve strategic effects short of significant armed conflict and in some respects short of kinetic conflict altogether. The problem is not theoretical or hypothetical, and there is an urgency attached to it given that some treaty allies feel exposed to such tactics. An additional argument is made for including the gray zone in a conception of integrated strategic deterrence: that deterrence is essentially indivisible. That is, effective deterrence of high end conflict cannot be separated from effective deterrence at the lower end if the principal task is to shape adversary perceptions – a task that is constant and continuous. This view of the gray zone would serve to broaden the deterrence problem set significantly.

A number of workshop participants argued against defining the gray zone as principally a deterrence challenge. Rather, this should be viewed as an arena for *competition* short of armed conflict where there is likely to be greater payoff from approaches that seek to resist and compete rather than deter. Moreover, there is risk in expanding the deterrence problem set; rather, what is required is a *more selective* approach to defining deterrence tasks for the armed forces and the interagency community. The challenge is to limit the application of deterrence as a strategy to those problems for which it is most clearly suitable and against which it is most likely to be effective.

As another example of the different possible conceptions of integration, some other participants viewed it less in terms of conflict management and more as a feature and driver of long-term competitive strategies *vis a vis* other major powers. This, too, is not surprising in light of real world events, given the re-emergence of rivalry with Russia and China, the high technology component of emerging military competition, and the recognized need to compete in a manner that preserves both strategic stability and U.S. freedom of maneuver, to the degree possible. This conception of integration merits further attention.

Why is a more integrated strategic deterrence posture important?

Since 2009, the United States and its allies have pursued a comprehensive approach to strengthening regional deterrence architectures and adapting them to 21st century purposes (as set out in the strategy and policy reviews of the time). This comprehensive approach encompasses a favorable balance of conventional forces; ballistic missile defenses, both regional and homeland; resilience in cyber space and outer space; and a "tailored nuclear component." The benefits to deterrence and assurance have been conceived by U.S. policymakers as largely cumulative. There has been little systematic thinking about how these sets of capabilities relate to one another in underwriting deterrence and defense – how one set can compensate for deficiencies in another, or how synergies can be exploited to create a toolkit that as a whole is greater than the sum of its parts in helping to manage crises, deter conflict and escalation, and generate more and better options for leadership.

As the toolkit becomes more diverse and sophisticated, this would be an important challenge even if our principal rivals were not moving in the same direction. But they are. Each in its own way, Russia and China are working toward a vision of strategic deterrence premised on the belief that future conflict will be “cross-domain” in nature and require the effective integration of a multi-dimensional set of capabilities. How much progress each has made is not fully clear, but both emphasize the cumulative benefit of capabilities for coercion and military operations that encompass hard and soft, kinetic and non-kinetic, and nuclear and non-nuclear means. Both also assert that integration can help them in a crisis (by presenting the prospect of unbearable cost to their adversaries), early in a conflict (to seize the initiative), and in the later stages of war (to manage the risks of U.S. escalation). Even absent the outbreak of war, the integration of strategic capabilities being pursued by the great powers represents, as noted above, an important element of long-term competition that must inform U.S. strategy development, plans, and investment.

Further, given that the United States in any confrontation with Russia or China almost certainly will be defending the vital interests of treaty allies, these partners will need to understand the emerging advanced technology systems both “blue” and “red” would field and seek to leverage. Especially if a more integrated approach to deterrence leads to new thinking about thresholds, “redlines” and proportionate response, the success of extended deterrence arrangements may depend importantly on a common appreciation of how a high-technology “cross-domain” conflict could unfold. And, as some allies develop advanced systems of their own (e.g., prompt strike, missile defense, cyber), a key task will be to harmonize concepts and capabilities to maximize the prospects for achieving decisive effects in support of deterrence and defense and minimize the risks of miscommunication and inadvertent escalation.

What are integration challenges for specific capability sets?

The workshop discussions indicated that thinking about discrete aspects of integration is uneven across the defense community, though clearly there is some useful work being done at the operational level.

US-Allied Integration. This aspect of integration is perhaps most mature, as it builds on decades of partnership in consultation, planning, capability development, and operations. These efforts in NATO and with allies in Northeast Asia continue apace today, in response to new or deepening threats. With South Korea and Japan there are mature dialogues on extended deterrence and assurance and a high degree of operational integration (in the case of South Korea) or interoperability (in the case of Japan). But further integration faces some challenges. In Korea, for example, improved integration requires addressing Seoul’s anxieties about potential gaps in policies, plans and capabilities to deter and respond to a variety of North Korean actions, up to and including the limited use of nuclear weapons. These anxieties concern, among other things, the amount of conventional combat power deployed on the peninsula (vice in Japan and on Guam), and the need for a tailored deterrence strategy toward the North supported by more robust strategic messaging. South Korea’s acquisition of independent means to strike operational and strategic targets in North Korea (e.g., “Kill Chain,” “Massive Punishment”) is one expression of these anxieties. The introduction of these capabilities may yield useful benefits for deterrence and new opportunities for US-ROK integration, but one can also envision the downside – a higher degree of risk and an emerging fault line in the effort to coordinate plans and military action to address North Korean aggressive acts.

In NATO, “integration” is not part of the lexicon surrounding the current effort to adapt alliance polices, capabilities, and organization in response to the new security situation in Europe. The discussion, rather, emphasizes the need for greater “coherence” among the various elements of NATO’s mix of capabilities. While NATO will not embrace the operational integration of its conventional and nuclear forces, its leaders recognize that strengthening deterrence requires more tightly linking these two elements of power in the perception of the adversary. Thus, NATO’s graduated response plans need to account more explicitly for Russia’s nuclear doctrine and capabilities and the challenges these could pose as NATO seeks to mount a conventional response to aggression. Likewise, exercises need to demonstrate more clearly the connection between conventional and nuclear deterrence and the Alliance’s preparedness to employ the full spectrum of its capabilities.

There are similar tasks to enhance coherence with respect to missile defense and cyber. NATO’s missile defense mission has long been oriented to threats from the Middle East, but the renewed challenge from Russia, not surprisingly, raises the question of how current and future capabilities can be integrated into the conventional defense of NATO territory in a confrontation with Moscow. NATO’s approach to cyber has fundamentally changed with the designation of cyber as an operational domain. Cyber now needs to be integrated into NATO’s graduated response plans. The larger question for the Alliance is whether its current Strategic Concept remains responsive to the new threat environment and the requirement for greater coherence across a more dynamic spectrum of conflict and capabilities. Some have argued that NATO needs a new “grand strategy” that better connects ends, ways and means.

Offense-Defense. The integration of strategic offense and defense has been the subject of analysis and debate since at least the establishment of the Strategic Defense Initiative in the mid-1980s. The context for this discussion has evolved to reflect the growing concern about regional threats. But in either respect, there appear to have been few conceptual or practical breakthroughs in understanding offense-defense dynamics in ways that directly influence our approach to deterrence and escalation. The workshop discussion offered three distinct lenses through which to view offense-defense integration going forward. At the level of great power competition and conflict, it remains important to consider offense-defense dynamics through the lens of strategic stability, traditionally defined. The challenge is to adapt this conception of stability to what will soon be a transformed technology landscape, one being shaped by the pursuit of new concepts for both offense and defense (e.g., hypersonic propulsion, directed energy, space-based BMD).

At the level of deterrence and defense *vis a vis* a regional power or rogue state, the opportunity and capabilities exist to better integrate offense and defense through a tailored concept for persistent surveillance, strike/interdiction, and active defense aimed at degrading the coercive power of ballistic missile forces. The goal is to better manage a threat such as North Korea’s growing missile force by limiting significantly adversary launch opportunities and enhancing the effectiveness of BMD systems.

Finally, within the missile defense mission, it is possible to achieve a higher degree of effectiveness and efficiency by adopting innovative operational concepts for "distributed defense" that build on the multi-domain warfare and distributed lethality doctrines being pursued by the Army and Navy, respectively. These innovations would lead to a higher degree of interoperability across air and missile defense systems and complicate adversary efforts to suppress these capabilities.

Conventional-Nuclear. The potential linkages between the conventional and nuclear dimensions of war were once a central consideration in U.S. strategy and planning for regional conflict. In the post-Cold War period, much of what had been learned about "theater nuclear planning" was lost. Only recently has this become a renewed focus of DoD planning in response to the changing nuclear threat landscape and heightened concerns about the ways in which a conventional conflict could escalate to the nuclear level. There is growing awareness of this problem at the geographical combatant commands, but there is much work to do. The goal is not to integrate the employment of nuclear weapons into conventional operations to support a war-winning strategy. Rather than lowering the nuclear threshold, the purpose of enhanced integration is to make deterrence more credible and adversary nuclear use (initial and follow-on) less likely. There are three main integration tasks.

- First, conventional campaigns against nuclear-armed adversaries should be designed to shape the adversary's calculus in the direction of nuclear restraint. This means looking at the campaign through the adversary's eyes, and understanding his perception of U.S. intent. In turn, this may require limiting U.S. or coalition objectives.
- Second, conventional campaigns need to be more resilient to the possibility of adversary limited nuclear use. Being prepared to operate in a nuclear environment requires understanding how the adversary may employ nuclear weapons and for what purpose. How could nuclear use disrupt operations? What adjustments and countermeasures are required to ensure campaign success? If the adversary can be convinced there is no likely operational benefit to be gained from nuclear employment, it may be possible to deter such attacks. If deterrence fails, a high degree of resilience can save lives and preserve leadership decision-making flexibility.
- Third, it is important to maintain limited, credible integrated options to respond to adversary nuclear use, and to make these known to the adversary. Absent such options, the adversary may conclude it can calibrate a limited nuclear attack to achieve important strategic and operational objectives while escaping a nuclear response. Response options would need to be considered in light of the ongoing conventional campaign and appropriately synchronized; limited nuclear responses

should not disrupt conventional operations. Existing U.S. nuclear forces, in particular bombers and tactical aircraft, possess the characteristics necessary for this mission.

Cyberspace and Outerspace. These domains are vitally important because they are critical enablers of U.S. military dominance through global ISR, automated C3, and precision strike. Potential vulnerabilities in these arenas first led to the idea of "cross domain deterrence," based on the fear that the United States could be deterred from resisting local or regional aggression if adversaries could use cyberweapons and counter-space operations to negate core U.S. advantages. If adversaries could disrupt or defeat key networks and space assets with some degree of ambiguity or plausible deniability, and using relatively inexpensive means, then the burden of escalation in response to potentially crippling attacks would fall on the United States. Some workshop participants argued that this idea continues to drive Russian and Chinese thinking, premised on their assessment that the United States is struggling with the question of how to manage deterrence and warfare in cyber and space and in fact lacks the will to fight in these domains.

Given their importance to U.S. operations, improvements to these capabilities tend to increase adversaries' incentives to pre-emptively neutralize them. And because there is great uncertainty about the likely effects of warfare in the cyber domain, in particular (in part because they are difficult to exercise), concerns about escalation and perceptions of vulnerability may persist among U.S. policymakers, planners and operators, and may contribute to a tendency toward self-restraint. In turn, this may contribute to perceptions in Russia and China of U.S. ambivalence about operations in these domains and reinforce their judgment that this is an area where aggressive, risk-taking behavior may be rewarded.

The workshop discussed a number of implications that could flow from this dynamic. Some participants pointed to the need for the United States to establish credibility regarding its willingness to respond forcefully to challenges in the cyber and space domains. The task is to lead Russia and China, in particular, to recalculate the risk associated with making such challenges. Progress toward this goal can be accomplished through words and actions that convey resolve and preparedness to impose meaningful costs and consequences. If various uncertainties argue against a policy emphasizing "in domain" retaliatory threats, then clearly there is a pressing need to think through how other capabilities can be leveraged for this purpose, and identify the principles or rules that should govern such a deterrence construct and its expression in plans and declaratory policy.

Others suggested the need to think more systematically and aggressively about adversary vulnerabilities, which are numerous. While Russia and China may see opportunities for advantage in perceived U.S. ambivalence about the cyber and space domains, they likely are also concerned about their own vulnerabilities in these areas as their capabilities become more advanced. More focused attention here could help shape an approach to deterrence based on the careful exploitation of mutual vulnerabilities. If vulnerability is a persistent feature of the cyber domain for all the major powers, one way to mitigate the chronic instability such a condition seems likely to produce is to move explicitly toward a regime of "mutually assured vulnerability." Such a regime would not be expected to serve as an effective deterrent against all types of attacks, but could be effective with respect to the most egregious attacks, such as those that could be directed against major economic, financial, infrastructure, public health, and nuclear command and control systems. Not all workshop participants were comfortable with the idea of mutual vulnerability along these lines.

"Black" and "White." From a deterrence standpoint, what is the most effective balance between capabilities that are visible and openly discussed or demonstrated and those that remain concealed and covert for any number of reasons? It is difficult, of course, to base a deterrence strategy on a capability that the adversary cannot see, know about, or understand. Deterrence requires some degree of revelation; "unknown unknowns" cannot be counted on to deter. But deterrence can also benefit from a degree of secrecy. Selective revelation (in whole or in part) of secret or black programs whose existence can be acknowledged could be an element of a strategy to heighten an adversary's sense of uncertainty and surprise, and to exploit perceived operational vulnerabilities. In considering such an approach, a key question is the tradeoff between an anticipated (or hoped for) deterrence benefit and the cost or risk to operational security. As a rule, this trade makes most sense when there is an expectation of altering significantly an adversary's strategic calculus and risk perception in favor of restraint. That is, the revelation should create an impact at the highest political levels, not just among operational, technical, or intelligence leaders.

This kind of approach can deliver potentially important benefits, such as degrading the adversary's confidence in his assessment of U.S. capabilities; signaling viable solutions or counters to problems presented by adversary forces or doctrine; devaluing significant adversary investments; and delivering a psychological shock that undermines other core adversary assumptions. There may also be limitations and risks from a deterrence standpoint: if there are only limited numbers of a revealed capability; if countermeasures can quickly be developed; if a demonstration of capability fails; if the adversary considers the revelation to be an escalatory act or otherwise reacts in an unanticipated or unwanted manner; or if an ally is surprised by a U.S. action. As an example, the current perishability of cyber accesses may argue against revelation for deterrence purposes. At the same time, it may be relatively easy to design low risk information operations that create adversary uncertainty about his own data.

Overall, maximizing prospects for success and mitigating some of these risks requires a sound understanding of the factors that would shape an adversary's response to the revelation or demonstration of an unexpected U.S. capability. It also requires the effective integration of operations and intelligence and finding ways to work around the compartmentalization that can inhibit the development and execution of innovative approaches to leverage black capabilities for deterrence and strategic messaging. Deception may also contribute to success. One participant cited successful examples of U.S. deception efforts during the Cold War with respect to strategic nuclear forces. Others cautioned that the use of deception carries high risk and should be considered very selectively as a complement to actions that rely principally on revealing actual capabilities. Choices about how much to reveal and when would be situation-specific and driven by immediate deterrence considerations. But it also may be useful to think about the way in which “slow reveals” over time could create advantages in long-term competition with key rivals.

What is needed to advance the development of integrated strategic deterrence?

“Demand Signal.” Ideally there would be a national strategy for deterrence that establishes an overall “ends-ways-means” approach to develop tailored or adversary-specific campaigns using all instruments of national power. As no such strategy exists, integration objectives and the importance of shaping deterrence along these lines should be reflected in existing high-level national and DoD strategy documents, and prioritized in key implementing guidance. This would constitute a demand signal to motivate the necessary work; such a signal does not exist today. In turn, creating a top-down push for integration in strategic deterrence requires articulating a practical framework or concept that conveys to leadership the need and the expected payoff and provides a basis for action at the working level.

Framework/Concept. The goal is to begin to operationalize the general aspiration associated with integration – stronger deterrence, better management of escalation risks, and improved non-nuclear options and decision time for leaders. Creating such a framework to support operational planning and crisis decision-making is not a simple task and our ambitions should be realistic. It certainly requires a better understanding of how adversaries are likely to execute integrated strategies of their own to both deter and manage escalation risks. Beyond this, a practical framework should strive to help policymakers, planners and operators better weigh risk and reward when facing cross-domain challenges and opportunities in regional conflict. This means “unpacking” and developing a set of working propositions around considerations related to thresholds and “redlines,” proportionality and reciprocity, norms and the laws of armed conflict, deterrence messaging, attribution, horizontal escalation, and strategic stability. These propositions need to be debated, tested and refined, and then formed into some type of “rule set” that can support deliberate planning in peacetime and adaptive planning in crisis and conflict.

Campaign Plans. An integrated approach to strategic deterrence must be embedded in deliberate planning activities, and can build on the innovations now being implemented in the Joint Strategic Campaign Plans (JSCP) process. This effort to remove some of the impediments to joint plans and operations should provide a foundation for developing *integrated deterrence campaign plans* that embody established principles of deterrence planning and encompass all instruments of national power. A rigorous strategic campaign planning process is the best hope to leverage the potential synergies among elements of the deterrence toolkit. Integrated deterrence campaign plans must be shaped by clearly articulated goals, sequenced courses of action, the innovative application of capabilities, and measures of effectiveness. Courses of action should reflect a government-wide assessment of the adversary perceptions to be influenced and the military and non-military means to achieve this. The DoD may bring the rigor of its planning processes to this challenge, but it owns only part of the solution set. The task of developing and implementing integrated deterrence campaign plans should not be confined to the DoD but ideally should be led by the White House through the coordinating role of the National Security Council.

Whether the NSC is well-suited to this task is a fair question, one that a number of workshop participants asked, pointing to their own (unsuccessful) experience trying to inject non-military concepts into guidance documents and planning frameworks developed by the DoD. Others expressed a broader concern about the degree to which the deliberate planning process can anticipate the requirements of an integrated set of deterrence actions in a crisis or conflict. In this view, integration of the deterrence toolkit might best be done "on the fly" – leveraging real-time leadership guidance, the experience of senior operators, and well-established crisis management practices. To a number of participants, this did not seem a prudent approach given the likely stresses and complexities of a future operating environment; a deliberate planning process (complemented by wargames and exercises) at least forces policymakers, planners and operators to think about the problem in an organized way and rehearse the challenges. But caution must also be taken to avoid the other extreme – that is, an approach that seeks to finely calibrate the application of force across multiple domains through some kind of formula. There may be a place for "algorithmic warfare" that anticipates the precise conditions under which increasingly autonomous military systems should perform certain military tasks, but the challenges of a complex escalation scenario are dramatically different and place very different demands on decision-makers.

Policy/Posture Reviews. The ongoing Nuclear Posture Review, Ballistic Missile Defense Review, and other strategic reviews represent opportunities to recognize the integration imperative and advance the overall objective. While recommendations for the reviews were not a primary focus of the workshop, some implications emerged.

- The reviews should convey a sound approach to tailoring. In a multipolar security environment, the United States defines different strategic relationships with different actors and tailors deterrence tools to reflect these relationships. The reviews must provide or set conditions for a coherent approach to each actor across the separate domains.
- The reviews should convey a coherent set of declaratory policies that reflect the complexity of a multi-domain operating environment and preserve flexibility to apply different elements of the toolkit as needed.
- The reviews should stake out clear positions on key issues such as the role of regional deterrence architectures in integrating U.S. and allied efforts and providing assurance, and the role of the interagency community in supporting whole of government deterrence solutions. In these and other areas, the policy and posture reviews begin from inherited approaches that if not reaffirmed will need to be replaced by alternative concepts.

What are useful next steps? Going forward, integration should be viewed as an imperative in two important dimensions: as a necessary feature of tailored strategies to deter highly capable adversaries in a regional conflict context, and as a key element of the long-term competitions now developing with other great powers who will seek to "win without fighting" or place the burden of escalation on the United States. In the first dimension, the task ahead is to set conditions for implementing practical steps toward greater integration, e.g., gain a better understanding of how Russia and China may execute their own integrated deterrence strategies to achieve advantage; develop a practical framework or concept that can inform high level strategy and working level activities; advance integration through the deliberate planning process and the use of campaign plans; and leverage the ongoing policy and posture reviews to promote integration objectives where appropriate. In the second dimension, useful first steps are to conduct tailored net assessments for the key regions of concern (Euro-Atlantic, Northeast Asia) and to define the nature of the emerging long-term competitions with Moscow and Beijing. Here, there may be benefit to revisiting work from an earlier era that focused on the development of competitive strategies.