LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-ABS-670206

Cross-Domain Deterrence Seminar Summary Notes.pdf

R. J. Vince

May 1, 2015

Cross-Domain Deterrence Seminar

November 18-19, 2014
Lawrence Livermore National Laboratory
Summary Notes

Introduction:

Lawrence Livermore National Laboratory (LLNL) hosted the Cross-Domain Deterrence Seminar on November 18-19, 2014, in Livermore, CA. The seminar, sponsored by LLNL's National Security Office (NSO) and hosted by the Center for Global Security Research (CGSR) and Z-Program, was designed to foster discussion on the interplay between nuclear deterrence, advanced conventional weapons employment, cyber warfare and contested space, and the impact of that interplay on the decision calculus of potential adversaries. The seminar benefitted greatly from the participation of a broad range of distinguished speakers from government, industry, academia, national labs and think tanks whose backgrounds covered the spectrum of conventional, nuclear, space, and cyberspace domains (attendance list provided at end of summary notes). The seminar was judged highly effective by participants; a follow-on is scheduled for November 17-18, 2015. Please provide comments and questions to Bob Vince at Vince1@llnl.gov.

The seminar was organized as a series of unclassified briefings and panel discussions on Tuesday, November 18th, followed by a series of classified briefings on Wednesday, November 19th. The panels on Tuesday included:

1. A Historical Look at Concepts of Cross-Domain Deterrence;
2. Competing Concepts of Cross-Domain Deterrence;
3. Considering the Role of Space and Cyber in Deterrence;
4. A Global Perspective; and,
5. Charting a Path Forward.

Below is a brief summary of the panel presentations and discussions from session held on Tuesday, November 18th. Significant editorial license is herein taken in order to preserve speaker anonymity and gather comments around common themes to improve flow and readability. While the goal of the editorial process was to preserve the original content of speakers' comments, inadvertent changes may have occurred due to context and timing that was difficult to capture or interpret; for this, the editor apologizes.

This summary is not a consensus. It includes multiple points-of-view on complex, interrelated issues.

The classified briefings and discussions of Wednesday, November 19th, will not be summarized.

Summary of Opening Comments:

Yesterday's challenges did not predict the challenges of today and certainly will not predict the challenges of tomorrow. More importantly, the challenges of tomorrow will not be answered using the tools we have today. Potential adversaries are taking advantage of rapid advancement and increasingly global availability of science and technology and are moving forward. The DOE/NNSA National Security Labs are developing both the science and technology tools and the

future leaders needed to address the challenges of tomorrow. This seminar was an opportunity to draw a broad community of expertise into the multidisciplinary environment that LLNL continues to rely on to develop creative solutions to national security challenges – in this case, the challenges to deterrence posed by rapidly evolving cross-domain threats. Participants were encouraged to contribute freely – on a non-attribution basis under Chatham House rules.

Panel One - A Historical Look at Cross-Domain Deterrence:

Cross-domain deterrence has been defined many ways; for this discussion an initial definition was proposed as a starting point:

> "The act of deterring an action in one domain with a threat in another domain, where the domains are defined as land, under the land, at sea, under the sea, in the air, in space, and in cyberspace, and may use economic sanctions and other diplomatic and political tools."

Deterrence – dissuading someone from acting before they act – needs to be clearly delineated from compellence (coercive diplomacy) – persuading someone to stop acting after they've acted.

Cross-domain thinking is not a new concept and was in play long before the nuclear age. George Quester's book, "Deterrence Before Hiroshima," analyzes pre-nuclear age theories and provides examples. Two of the key concepts that are central to nuclear deterrence originated not with the nuclear age, but with the advent of air power – the concepts of counter-value strikes and offense advantage. Before the end of WWII, the air war made it clear that counter-value strikes could be used to achieve military, or counter-force, objectives. There are historical examples illustrating how preemptive strikes were used to gain offense advantage; one such example is Pearl Harbor, which can be viewed as an attempt by Japan to preemptively degrade the US' ability to execute an offensive air campaign in Japan and the Western Pacific (which would have been more effective had US carriers been in port).

There are many historical examples of cross-domain thinking since WWII:

- NATO relied on the threat of nuclear use to deter superior conventional Soviet forces.
- Soviet advances in space and ballistic missile technology threatened the credibility of US/NATO nuclear forces by providing Soviets with means to threaten the US homeland in response to US/NATO nuclear threats in theater.
- A [veiled] nuclear threat was used to help bring a negotiated end to the Korean War hostilities after what was essentially a stalemate in the conventional conflict.
- The US used actions in multiple domains – a naval blockade, threat of an air campaign, and changes in nuclear posture – to compel the removal of Soviet missiles from Cuba while deterring an escalatory response through local conventional naval superiority and global strategic nuclear retaliatory capabilities.
- Diplomatic pressure has been used to prevent North Korea from delivering banned arms by sea.
- Economic sanctions are routinely used to deter conventional aggression and nuclear proliferation.

In all of the historical cases, US policymakers consistently sought to adopt measures that would be effective with minimum likelihood of provoking retaliatory escalation. There is some historical evidence that cross-domain actions may appear escalatory to some adversaries.

Cyber threats and the potential to produce physical damage and loss of life through cyber means have expanded the scope of thinking and actions in cross-domain deterrence. The cyber attack against Iranian centrifuges was escalatory in the cyber domain; Iran has since stepped-up their

cyber attacks, and it may have emboldened others to become more aggressive in the cyber domain.

The cyber attack to destroy Iranian centrifuges was not intended to deter Iran, but rather to delay the Iranian nuclear program. However, the effect the attack created – delaying Iran's enrichment program – provided more time for economic sanctions to take effect and increased pressure on Iran to return to the negotiating table. This is an example of how cyber attacks may be used in conjunction with actions in other domains to create deterrence effects.

The cyber attack on Iran's centrifuges may also have been intended to assure Israel and deter them from using military force to attack Iran – essentially a cross-domain deterrence and assurance action.

Panel Two - Competing Concepts of Cross-Domain Deterrence:

The cross-domain deterrence problem raises a host of questions:

- Why might an actor engage in a cross-domain asymmetric response in the first place?
- How do we signal our intentions in one domain with action or inaction in another domain?
- Does signaling become easier or harder with additional domains?
- What are the potential impacts on alliance management?
- Given the complexity of the issues, is it even possible to craft a cross-domain strategy or is it simply too difficult a problem to conceptualize?

There is a lot of nervousness around the coming-unglued of the international security architecture, and, like in the movie *The Big Chill*, we are starting to realize that, long after the euphoria at the end of the Cold War, we have not achieved what we set out to do and are feeling inadequate, insecure, and discovering that everyone else shares our angst and uncertainty about the future. It's like musical chairs in a political, economic and security sense – everyone is nervous about what to grab-onto when the music stops. Taking our traditional approach of looking over our shoulder to see who is following our path, we discover that people are not following us; however, they are breaking new ground, taking alternate paths that are complicating matters, especially in the cross-domain area. Given this ungluing of the international security architecture, we will likely see more polarization on the nuclear question. Some people are pressing for global zero by a date certain, like 2030; others are saying it is much farther down the road and we need to figure out how to steer the ship in stormy waters right now. We will likely see polarization on that issue and cross-domain will play into that debate as well. There are many factors that must be considered as we develop new approaches to deterrence:

- Cross-cultural issues are very important. Many political leaders from diverse countries are making the same speeches, but are thinking about the problem in very different ways.
- Risk assessment technology is emerging along with new work in sociology, economic analysis, and behavioral psychology, but the cultural dimension is still a very uncertain one; we need to find ways to deal with that.
- The geography problem is back and cross-domain issues play heavily; Estonia and Georgia, for example. Are cyber and space domains global or local, or are they geographic at all?

Nuclear is different – it's part of the message, but it's also reality. Deterrence is not just nuclear – it is strategic and, by definition, strategic crosses and engages multiple domains. So, cross-domain has to play in the geopolitical environment. Much of the cross-domain discussion is based on the premise that there are certain similarities between regular (nuclear) deterrence and cross-domain deterrence, but opinions vary on whether all or none of the classic deterrence

lessons apply. There are examples that show similarity between some domains, but do those similarities matter?

The strategic significance of cross-domain effects is related to what levels of destructiveness are possible in a particular domain. Potential nuclear destructiveness of today's stockpile is much less than it was, but is arguably many thousands times more than conventional weapons. Even given a particular set of capabilities, strategy and intent play a large role in determining how destructive that set of capabilities may be. For example, in the nuclear domain, flexible response and minimum deterrence approaches generate very different damage scenarios for the same stockpile size, based on the targets and proportionality of responses. A minimum deterrence strategy generates more damage with a smaller stockpile because of the targets that need to be held at risk to achieve its strategic ends (which tend toward counter-value).

There is concern about increased morphing in the policy debate – are capabilities needed more for deterrence or more for warfighting? These alternatives have never been entirely binary, not either/or. Credible deterrence has always been in-between, with constructive internal tension. It's becoming more so, not only in the upper realms of escalation, but even more in the lower realms, especially the classic problem of crisis versus conflict. Our willingness to consider something an act of war in the cyber domain is much more nebulous than in the nuclear or conventional domains. With all this complexity, it is helpful to have flexibility, agility, and diversity.

We ought to examine a hypothesis – In a world with fewer nuclear weapons and more players, cross-domain factors will weigh more heavily in what is already becoming a rather complex multidimensional geometry of escalation. One of the real challenges for policymakers is the blurring of concepts and categories that make simple rule-based decision-making more difficult. Whether or not the hypothesis is correct, it provides an opportunity to do some fresh thinking about deterrence. We are in a period of generational change with more young people coming into the discussion. With the world changing as it is, we have an immense learning curve for which we need fresh brainpower, but we also have a huge forgetting curve, particularly with regards to nuclear deterrence. It might be useful to look for insights into the cross-domain problem by taking some of the old data and giving it to the new thinkers and taking some of the new data and giving it to the old thinkers and comparing results.

Minimum Deterrence

Since President Obama's Prague speech, there have been a plethora of proposals for Minimum Deterrence and much written on the topic - 9 books, 25 institutional reports, 150+ articles in on-line and print journals. All the proposals are built on a common set of 9 premises. These premises are accepted to be true and are used as the basis for arguments:

1. Deterrence will function reliably and predictably at low levels.
2. Conventional forces can meet targeting duties.
3. Russia and China are not US enemies, nor will they be in the future.
4. Nuclear weapons are irrelevant to today's most pressing security concerns (WMD attack).
5. Deterrence considerations alone determine the size and composition of the nuclear force.
6. Ballistic missile SSBNs will remain invulnerable for the foreseeable future.

The last three relate to benefits that minimum deterrence is asserted to provide.

7. Risk of accidents directly correlates with stockpile size – fewer weapons makes us safer.
8. By reducing the stockpile, we serve nonproliferation efforts and goals.
9. Defense spending can be reduced by nuclear reductions.

Minimum deterrence proposals typically "connect-the dots" between various premises in order to come to the conclusion that the US should reduce the nuclear stockpile to very low numbers.

However, some have observed that all the premises upon which the minimum deterrence proposals depend can be shown to be demonstrably false. Indeed, available evidence indicates otherwise, or that the premise is not a certainty (for example, SSBNs being invulnerable for the foreseeable future).

Takeaways:

- Premises that conclusions are built upon need to be valid and dependable - based on empirical evidence, historic examples, analysis and logic – red teaming could be valuable.
- US views on what should assure and deter may be erroneous; deterrence is in the mind of adversary leaders and assurance in the mind of our allies.
- We can't guess what is in the future. Minimum deterrence does not deal well with uncertainty. At minimum force levels, you lose flexibility and resilience – valuable attributes for mitigating risk in a dynamic and uncertain future environment.
- "There are two ways to be fooled. One is to believe what isn't true; the other is to refuse to believe what is true." -- Kierkegaard

Escalation

There are a range of escalation philosophies that describe an actor's resistance to nuclear use as a function of conflict intensity:

- Tripwire – which rely on early use to bring a quick end to the conflict;
- Warfighting – which can result in early and frequent, sustained, use throughout a conflict;
- Psychopolitical – which have a characteristic of episodic or punctuated use in a repeated attempt to terminate the conflict; and,
- Extremis – which rely on nuclear weapons only as a last resort.

To determine the type of strategy a particular nation relies on, one must examine a broad range of characteristics including leadership, strategic culture, forces, posture, doctrine, targeting, NC2, declarations, etc. Countries with limited conventional capabilities may tend toward the tripwire end of the spectrum, whereas countries with a wide range of capabilities to bring to bear may tend toward the extremis end. There is a danger zone when adversaries have markedly different escalation philosophies, especially when they don't realize it. This "asymmetry of wills" can lead to miscalculation and unanticipated escalation; declaratory policy can play a role in minimizing the chance of miscalculation. Also, risk and stake assessments are not static – what starts out as a peripheral interest might become a vital interest, especially if nuclear threats or use occurs.

Deterrence thinking came to academic maturity with the works of Brodie, Schelling, and Kahn. Kahn's escalation ladder helped frame cold war thinking on deterrence and escalation control. However, Kahn's escalation ladder is inadequate for today's environment, which must consider multiple domains of escalation. So, how do you visualize escalation across multiple domains?

There are various escalation geometries, from a singularity (threshold), to linear (escalatory ladder), to 2D (escalatory lattice, taking into account other domains), to 3D (escalatory space, taking onto account geography – homeland, continent, ally, etc.), to Escalatory Vortex (adding timing/sequence), and "N" higher orders that might be referred to as Escalatory String Theory – taking into account culture, psychology, etc. Since "N" can grow very large, making decisions unnecessarily complex, what is the Nth significant dimension of deterrence?

While Herman Kahn's escalation ladder has cross-domain elements, you may want to visualize cross-domain deterrence using a number of parallel escalation ladders – akin to a graphic equalizer. Using that analogy, not all bands (domains) are equal; some may be taller than others. In theory, you can add thresholds in each band – harassing actions, armed conflict, and major

war. The analogy suggests that there may be cross-domain equivalents that are roughly comparable on an intensity-of-conflict basis.

If you chose a parallel ladder representation, how would you operationalize it? It seems there is a potential for developing an algorithm to quantitatively test propositions for controlling escalation risk in a multiple-ladder scenario. Escalation risk could be a product of a rung, crossing a threshold, and expanding the conflict into another domain, divided by a fear factor. The fear factor represents the degree to which an adversary feels you have more capability in reserve and are prepared to use it; that fear factor reduces risk that an adversary will escalate.

It might be helpful to try a test case. Better yet, we ought to use digital gaming technology to run many games to test many variables for analysis of strategies, capabilities and cross-cultural behavior. Build out escalation ladders for the US and various adversaries. Think about cross-domain equivalence using subject matter experts. Think about thresholds in each domain. Develop and test some propositions on where the risks lie. Much of the work would have to be done in the context of war games – like DEGRE. Socialize the results with planners, decision makers, and operators. There will likely be a lot of interest in figuring out how to generate new rungs on the ladder in times of crisis to stay below thresholds and how to gain agreement on where the thresholds are.

The escalation vortex has been proposed as an alternate to the escalation ladder for visualizing escalation dynamics. There are "equivalent" levels of conflict intensity across domains that are represented by the height that has been reached on the vortex surface. Different escalation philosophies can be visualized as different types of escalation surfaces that build across domains as a conflict evolves. The capabilities actors have to respond to different levels of provocation in each domain can also be represented, which can help illustrate vulnerabilities or potential opportunities when developing strategies to manage escalation. The vortex also allows visualization of tools available to control escalation at various levels of conflict intensity – for example, the resilience of the triad for managing first strike stability and escalation.

When escalatory ladders overlap (different means produce ends in the same domain), people behave differently and you get nonlinear responses to actions – for example nuclear EMP has effects in multiple domains and could be considered to be a nuclear, or electromagnetic, or quasi-cyber attack. This type of behavior will confuse rule-based approaches to managing escalation. For example, during Desert Storm, the US attack on Iraq's electric grid had a counter-force objective – but was criticized for its impact on people and considered by some to have had disproportionate counter-value even counter population effects. As these problems become more complex, we need to do more gaming to understand interactions and effects.

Current cross-domain discussions tend to focus on the domain of the originating action (the means) rather than the consequences of the action (the ends). Since deterrence and assurance are in the minds of adversaries and allies, and the psychological effect is dominated by the ends, should cross-domain considerations place more emphasis on the ends than the means?

It was noted that while the term "Cross-Domain Deterrence" is widely used, it may be falling out of favor in the some sectors. However, a new phrase has not yet replaced cross-domain deterrence to describe a holistic coordinated deterrence across multiple domains.

Panel Three - Considering the Role of Space and Cyber in Deterrence:

The biggest threats to deterrence and conflict going forward are the Four M's – Misperception, Misunderstanding, Murphy's Law and Mother Nature. Space and cyber domains are different and less predictable than nuclear and conventional domains. Monitoring behavior and doing damage

assessments can be challenging, especially in the cyber domain. The effects of cyber and space attacks can be much more unpredictable than conventional or nuclear attacks. The larger the scope of use, the more unpredictable the effects due to the high level of interconnectivity.

Cost to develop offensive space capabilities are reasonable given the benefits the capabilities provide – offensive space can counter capabilities that require much larger investments to develop. The same can be said for cyber. There is an inherent risk to strategic stability whenever modest investments in offensive capability can create disproportionate danger to an adversary; it makes preemptive strikes look very attractive. The ability to attribute space or cyber attacks to a particular adversary are also important and the lack of hard attribution (plausible deniability) can lead to instability.

Limited attacks are very tempting and at a low level are very likely to happen – will there be a mechanism to prevent rapid escalation? In conflict, it will be tempting to go all-in because the adversary has little time to "button-up" and retaliate. The temptation to escalate in cyber or space is balanced by uncertainty and risk aversion. Actors today are somewhat self-deterred from acting in some of the new domains because of uncertainty in the magnitude of the effect that might be created by doing so. Uncertainty of adversary cyber capabilities, coupled with rapid technology evolution that may cause an attacker to be uncertain of their own attack effectiveness, creates a risk aversion firebreak. An "island of stability" is created when actors underestimate their capabilities and overestimate the capabilities of their adversaries; that island is probably more pronounced as the level of attack being considered becomes more "strategic."

As yet, there is no comparable corollary in space or cyber domains to the resilience of the nuclear triad. Resilience should be a goal for space and cyber. However, if resilience is too effective, it may create a moral hazard – creating a feeling of invincibility and eroding the will to exercise restraint.

Growing threats to space and cyber are significant from peers and other state actors. Cultural and political perspectives are important, so regional experts must be engaged in deterrence discussions; deterrence without regional expertise is pretty sterile.

Space

The US National Security Space Strategy, 2011, describes space as an increasingly congested, contested and competitive environment.

There is growing risk from countries developing the capability (and sometimes a demonstrated intent) to challenge our supremacy in space that has important implications for the role of space in deterrence. Deterrence does not operate uniquely in space or any separate domain – it operates across domains and in the minds of potential adversaries. Space policy and posture can contribute to deterring attacks on space assets through a multilayered approach that complicates adversary decision-making. Deterrence in space can easily fail, with important implications for our warfighting capabilities in other domains and overall deterrence and crisis stability. More important than deterrence is resilience – the ability to support mission success despite interference in our space capabilities. We will need to be able to operate in a space environment that contains the equivalent of IEDs.

From the 2011 US National Space Policy, "the US considers the use of space vital to its national interests." If it's really vital, then the US should be prepared to go to war to protect that capability. But, is anyone going to go to war to protect space assets? The idea that any President would automatically use military force in response solely to interference with space capabilities is both foolish and dangerous. At a time when the credibility of red-lines has come into question, the idea

of a red-line in space is particularly incredible. Activities in space may be the least relevant factor in decisions on the use of force. Decisions on the use of force will be based on actions that occur on earth, where hostile actions are likely to have the biggest impact on US and allies' security.

It is wrong, even dangerous, to think in terms of space deterrence. Wrong, because space operates across domains and deterrence is in the minds of potential adversaries. Dangerous, because it leads to bad decisions, like decisions to stick with vulnerable space systems and architectures that invite attack. Decisions to create declaratory red-lines that lack credibility in peacetime and risk miscalculation in crisis or war are also bad decisions. Deterrence has a role, but it is a lot more nuanced than what was captured in the 2011 Space Policy. The DoD Directive (DoDD 3100.10, Oct 2012) that implements the 2011 policy is more nuanced. It advocates a multi-layer strategy intended to create doubt in an adversary's mind about the potential effectiveness of an attack, the international response to an attack in space, and the potential for miscalculation and unintended escalation. It includes:

- Support for development of international norms of responsible behavior that promote safety, stability and security of the space domain;
- Building coalitions to enhance collective space security capabilities;
- Mitigating the benefit to an adversary of attacking US space assets thorough resilience and the ability to operate effectively in a degraded environment; and,
- Possessing capabilities to respond to an attack on space assets in an asymmetric manner using any or all elements of national power.

The strategy is intended to make adversaries think twice about taking hostile action in space and encourages those decisions to be thought of as strategic decisions for heads of government, not tactical decisions to be made by forces in theater.

Deterring an attack on space assets may fail because attacking a space asset may seem trivial compared to other forms of confrontation, and it may be inviting if judged possible to do in a manner that provides little warning, is hard to attribute, and avoids lasting damage. When successfully attained, resilience in space will provide for mission success even when space capabilities are under attack.

Cyber

Some people warn of the potential for a Cyber Pearl Harbor. Most US impressions of Pearl Harbor bring to mind a bolt-out-of-blue attack, strategic surprise and setback. But, that is not an accurate characterization – it was not a surprise and had even been previously war-gamed. The US positioned the fleet forward to show US strength with the strategic intent to deter Japan from attacking. But, by moving the fleet forward, it was within Japan's reach. Japan's preemptive strike was an attack on our deterrence strategy and was an attempt to encourage the US to reach a negotiated settlement rather than rebuild the fleet and pursue the conflict. What the Japanese attacked at Pearl Harbor was our strategy – and that is the key insight into the relationship between Pearl Harbor and cyberspace. What would be the intent of a cyber attack – would it be standalone or in combination with actions in other domains?

We think about cyber and conventional domains separately, which is wrong. We are a cyber-enabled conventional force. Cyber attacks will be used to cripple conventional forces. If we experience a cyber attack, it will be part of, or a precursor to, a real kinetic fight and may be used to try to delay the US' ability to respond in a fight. It will not be hard to attribute – it will be used to defeat our deterrence strategy and present us with a fait accompli. If they are successful in creating a fait accompli, we will have to decide to fight our way back and perhaps escalate the conflict.

To strengthen cyber deterrence, one should break the distinction between warfighter and cyberfighter; reduce opponents' confidence in a cyber attack; bolster backup systems and increase local autonomy; and, present changing conventional deterrent threats to make it difficult to link cyber attack with a predictable impact on conventional capability.

Panel Four - A Global Perspective:

Regional capabilities (capabilities deployed in theater) are key to extended deterrence and assurance of many allies – especially Japan and South Korea. There are asymmetric stakes and pain thresholds between big and small actors that play significantly in their decision calculus regarding escalation and nuclear use.

China

The Chinese see themselves as taking a defensive posture, denying the US the ability to project power into their sphere of influence by relying on sharp pointed tools that both deny US capabilities and produce psychological effects. Cross-domain challenges from China will grow as they grow their capabilities in different domains – presenting them opportunities, but also creating vulnerabilities as they become more reliant on those domains.

Developing a multi-domain strategy to address potential threats from China will be challenging. The strategy must consider whether to respond in a proportional or asymmetric manner and how to balance declaratory policy with intentional ambiguity. There is the potential for a mixed strategy, where the declaratory policy and proportionality for each domain are tailored to the strength and resilience of capabilities in that domain.

South Asia (China, India, Pakistan)

In South Asia, deterrence operates largely through domain-specific escalation dominance. South Asia is a three-body problem and, using a physics analogy, it's not possible to prove stability for the three-body problem. In South Asia, Pakistan developed its nuclear force to counter India's superior conventional threat. India developed its own nuclear force, primarily to deter China. However, Pakistan often interprets India's advances in nuclear capabilities to be directed at them. Opportunities for misunderstanding and miscalculation in this three-body problem abound.

Both India and Pakistan have needed US intervention to bring crises back into stasis. However, they don't welcome US intervention that has prevented their ability to respond to provocation in the past. Partially in response to US diplomatic interventions, India changed its strategy and posture to "Cold Start," with a million-man standing army, to enable it to respond in a rapid way before the US can intervene. This resulted in changes to Pakistan's nuclear posture and its declaration of intent to deploy tactical nuclear weapons. This strategy, posture, and dynamic can lead to rapid escalation in a crisis and increase pressures on critical decision-makers. The US needs to engage India and Pakistan as partners before a crisis occurs in order to discuss actual conflict parameters and reduce the pressures that could lead these two regional powers to act precipitously.

Russia

There are a number of issues in US/NATO and NATO/Russia relationships that require continued attention:

- Deterrence and extended deterrence are "not in a good way" with the US and NATO. The US has globally shown itself not to be credible in certain areas; in particular, by failing to take action when adversaries have crossed stated red-lines. And, while everyone else is

modernizing their nuclear forces the US fails to do so, raising questions about how effective the US' cold war arsenal and warhead capabilities might be in potential future conflicts. The US needs to consider how these concerns might motivate our allies and the potential effect on nonproliferation. And, might Putin or someone else think now is as good a time as any to break the back of NATO?

- A resurgent Russia, not Iran, needs to be the focus of NATO. Russia is a strategic competitor and adversary of NATO. Deterrence has to be at the core of NATO's identity and deterrence of Russia is being eroded due to NATO's failure to respond to Russian provocations.
- Russia has demonstrated a pattern of disregard for international norms and treaties; NATO needs to internalize that behavior and prepare to respond.
- Russia has taken steps in intermediate range missiles that need our attention. We need to show ourselves to be flexible on missile defense and not in the way that Russia would prefer. We may need to think about deploying offensive conventional missiles to counter the developing Russian capabilities. Land attack missiles, for example, potentially coupled with smaller nuclear warheads, may have an important role. To enable such a move, we need to review our current opposition to new systems. We also need to be thinking about our next strategic concept – maybe a new NATO DDPR in response to Russia's revised doctrine.
- Russia's military is becoming more robust and forces are modernized, including weaponization of information via propaganda and control or seizing of media outlets. Although Russia is becoming stronger militarily, in some ways it is still very weak. The perceived need to take action as a face-saving measure, combined with demographic, economic and energy trends, translates to risk for deterrence. A declining power may take impulsive thrashing actions to distract from its decline.
- It may be difficult to deter Russia's aggression in cyber, information, and deception campaigns, but those campaigns will likely be used to support a conventional invasion. NATO needs to think about deterrence in those domains and focus on how to prevent the follow-on invasion to prevent a fait accompli, which is the certain objective of cross-domain actions. Deterring an invasion likely requires forward deployment of US or NATO forces into areas that Russia might choose to invade.

Panel Five - Charting a Path Forward:

Deterrence is a fairly limited notion of influence and, in reality, what we are often trying to accomplish is compellence or coercion, so it is more useful to think broadly about influence. (There was general reluctance among seminar attendees to entertain a shift away from the more common, narrow definition of deterrence. On the other hand, insofar as deterrence is in the mind of the adversary, is it worthwhile to consider potential adversaries' interpretations of the concept of deterrence – China's, for example?)

Strategic bargaining is a contest between sets of ends and means. Traditional deterrence theory focuses on the ends and usually assumes the means are nuclear. Cross-domain deterrence focuses more on the means – including options, combinations, and tradeoffs between different means. Combined arms - air/land/sea battle - is an example of thinking about the means and represents cross-domain thinking. Cross-domain deterrence is a broader problem because there are more means available, more linkages between them, and more actors with different portfolios of capabilities and vulnerabilities. How do the increasing number actors and means available for political influence affect deterrence in theory and practice? Can we develop rules of thumb (similar to combined arms) that capture "best response" actions to threats in different domains?

War is politics by many means and deterrence is a cost-effective way to achieve policy objectives. There are three objectives of deterrence:

1. Reduce risk of escalation/war;
2. "Win" the policy dispute; and,
3. Minimize cost of achieving the first two objectives.

If war is the product of different expectations about who is stronger in a conflict, then deterrent actions reduce the risk of war when they reduce opponents misconceptions about who will eventually prevail. Escalation reflects an effort to deter or compel an adversary's behavior at lower cost due to uncertainty about what it will eventually take to prevail in conflict.

Cross-domain actions can contribute to strategic deterrence by altering the balance of power and/or reducing uncertainty about intentions. Contrast some possible actions in the air and land domains. Forward-deploying air power to a region alters the balance of power, but it does not signal stiff resolve because air forces can be quickly withdrawn. Introducing ground forces to a region may not significantly impact the balance of power, but it signals resolve to defend the territory. Both balance of power and resolve factor into deterrence and escalation calculus.

Crossing domains can alter the balance of power and may increase an actor's ability to prevail if conflict occurs. Cross-domain actions, or combinations of actions, can be used in an attempt to shift the conflict into domains where an actor has the advantage, to impose costs on an adversary, to limit adversary options, and/or to heighten an adversary's uncertainty about their ability to prevail. Eliminating adversary options may encourage them to back down or it may cause them to escalate in domains where they can still take action.

Cross-domain actions can lessen or heighten the risk of escalation. Actions lessen risk when they inform an adversary about the likely outcome of the conflict. However, they heighten escalation risk if those actions are seen as tentative and signal that escalation might prevail.

Can we develop a theory of cross-domain deterrence? There are limits to what theory can do, but we are acting on a theory when we make any decision in anticipation of consequences. There are historical data on the use of cross-domain effects that may be helpful to examine in the context of developing a theory of cross-domain deterrence. How might historical examples best serve as a basis for analysis to better understand interdependence of domains, multipolarity, and the use of asymmetric capabilities?

Prepared by LLNL under Contract DE-AC52-07NA27344.