2015 Cross-Domain Deterrence Seminar

Summary Report

CGSR

Center for Global Security Research

LLNL-TR-682064

LAWRENCE LIVERMORE NATIONAL LABORATORY

2nd Annual Cross-Domain Deterrence Seminar Report

Author: Anthony Juarez
Graduate Student Researcher, Center for Global Security Research, LLNL
MPP Candidate, Richard and Rhoda Goldman School of Public Policy, UC Berkeley

17 November 2015
Lawrence Livermore National Laboratory
Livermore, CA

Lawrence Livermore National Laboratory (LLNL) hosted the 2nd Annual Cross-Domain Deterrence Seminar on November 17th, 2015 in Livermore, CA. The seminar was sponsored by LLNL's Center for Global Security Research (CGSR), National Security Office (NSO), and Global Security program. This summary covers the seminar's panels and subsequent discussions.

Attendees and panelists came from diverse backgrounds in academia, government, industry, the national laboratories, and think tanks with expertise in conventional (sea, air, and land), nuclear, space, and cyber domains as well as the non-military instruments of statecraft. A number of foreign experts were included in the discussion as well.

This seminar was the second in what is expected to become an annual series of workshops to explore the challenges of deterrence in a changed and changing security environment. The inaugural event in November 2014 also drew a diverse audience to survey emerging thinking about the cross-domain problem. A summary of those proceedings is available at http://www.slideshare.net/LivermoreLab/summary-notes-47797997.

This year's seminar had two primary aims. The first was to assess progress in coming to terms with the new challenges of cross-domain deterrence over the last decade. The second was to advance new thinking on a couple of key challenges in the study of cross-domain deterrence (deterring cross domain coercion in Phase Zero and managing escalation cross domain). A key related objective was to define an agenda for further research and analysis by the interested community.

The seminar used four panels to address its intended aims:

1) Assessing our progress in thinking cross-domain
2) Thinking about cross-domain deterrence in phase zero
3) Managing escalation across domains
4) Defining a pathway to integrated strategic warfare

This summary is not intended to capture every seminar discussion point. It does include the ranging and multiple viewpoints on complex, interrelated issues and seeks to give a general overview of the conversations that took place during the seminar. As a complement to this summary, CGSR has also prepared a lightly annotated bibliography of materials discussed in the workshop. It is available at https://cgsr.llnl.gov/content/assets/docs/CDD_2015_Bibliography.pdf.

Executive Summary

While the community has made progress in addressing cross-domain deterrence's (CDD) definitional deficiencies, an authoritative definition for CDD remained elusive. Integrated strategic deterrence, however, has begun to emerge as a new paradigm to frame U.S. and foreign thinking on deterrence. Significant thought has been given to the integration of state capabilities in Washington D.C. and the capitals of other world powers, with the latter arguably further ahead in the design and implementation of strategic integrated deterrence and compellence strategies.

Specifically, the Russian Federation and People's Republic of China have already devoted energy to understanding how to integrate their respective bureaucracies and national resources to deter and compel adversaries in order to achieve their strategic goals. These states have moved beyond the preliminary planning stages and are engaged in implementing strategic deterrence strategies.

Furthermore, many challenges remain before a complete understanding of how deterrence and escalation across different domains might work in practice, specifically in regards to space, cyberspace, and nuclear weapons.

Beyond the challenges posed by understanding the role of CDD, the escalation risks it might pose, and the integrated strategies of potential adversaries, one key question remains: How should the U.S. respond to the integrated strategies of its potential adversaries, Russia and China? In deciding whether to respond in a symmetrical or asymmetrical manner, U.S. policy makers must consider that the institutional hurdles to integrating U.S. strategic capabilities are significant—in the words of one of the seminar's panelists, the U.S. is not organized for the integration of capabilities.

Panel 1—Assessing Our Progress In Thinking Cross-Domain

Defining the Problem

The day's first panel was tasked with assessing the progress made over the past year in addressing cross-domain deterrence (CDD). The panelists and audience members, however, quickly established the community still struggled with an authoritative definition for what constitutes CDD. Further, some argued that CDD may only feel like a fresh approach to deterrence because we are grappling with relatively new deterrence challenges—cyber and counter-space—but the problem remains the same: deterring adversaries from taking specific acts with our current strategic toolkit.

Touching on a theme that would run through all the day's discussions, conference participants underscored the urgent need to better tie our national means to further the pursuit of US strategic interests—especially in the space and cyber domains. Panelists and audience members argued Moscow and Beijing have already begun to think about and implement policies along these lines.

This panel addressed the progress the U.S. strategic community has made in thinking about CDD and its utility in addressing U.S. strategic interests. Identifying which security challenges CDD can help the U.S. address remains a contentious process. Some participants questioned if the true purpose of CDD is the deterrence of strategic threats or the integration of the instruments of U.S. power, noting there is nothing new about warfare being conducted in multiple domains simultaneously. Others questioned whether "deterrence" is the right frame of reference, on the argument that conflict may occur in many domains and orchestrating effects to achieve U.S. deterrence objectives may be significantly complicated.

Adversary Perceptions

Conference participants highlighted adversary analysis as an important future area of research and suggested that fruitful CDD work in the coming year should focus on scenario analysis.

Comparing Cross-Domain Effects

When crossing domains, a challenge exists in terms of comparing the consequences of actions in different domains and assessing inter-domain proportionality. Pursuing a better understanding of proportionality among domains does not indicate that U.S. responses should *always* be proportionate. Though it is important to know what a proportionate response might be, it is imperative to know when any potential response will be perceived as disproportionate to avoid inadvertent or accidental escalation. This is an area for future work given the analytical tools available to assess proportionality.

U.S. Space and Cyber Asymmetric Vulnerabilities

One of the primary drivers behind thinking in terms of CDD is the importance of the cyber and space domains to terrestrial U.S. military operations. Participants asserted that U.S. space and cyber systems are resilient against low-level attacks, but the potential for catastrophic attacks in these domains and an absence of credible U.S. deterrent threats to protect these assets creates asymmetric U.S. vulnerabilities in these domains relative to its potential adversaries.

The Nuclear Component

Disagreement abounded regarding the role of nuclear weapons in any future cross-domain contingencies. Arguments regarding the danger of breaking down longstanding firebreaks between nuclear and conventional force were juxtaposed against those arguing that nuclear weapons remain the only symmetric response to nuclear as well as large-scale chemical, biological, and cyber attacks that could cripple large segments of domestic infrastructure. Since Cold War-era nuclear effects research focused primarily on blast effects, new research could usefully focus on understanding the potential electromagnetic pulse effects, the effects of secondary fires created by nuclear weapons, and other non-blast nuclear effects to better understand nuclear weapons' role in limited regional contingencies. A broader discussion of the necessary and appropriate role of nuclear threats in deterring adversary exploitation of U.S. vulnerabilities in cyber and outer space would also be useful.

Adversary Cross-Domain Integration

Potential U.S. adversaries currently practice broad-spectrum whole-of-government strategies that integrate military and non-military instruments of state power. There is a disconnect between the offensive and coercive strategies potential adversaries employ and how some argue the U.S. thinks about deterrence—as an often passive and defensive construct. Evidence suggests these adversary strategies are carefully considered plans rather than tactical decisions made on an ad hoc basis. Recent developments in foreign military doctrine and strategy suggest to some seminar participants that U.S. rivals are more prepared for CDD and compellence than the U.S. This signals the need for a crosscutting, holistic U.S. deterrence strategy that understands and integrates full-spectrum U.S. capabilities and instruments of state power.

Panel 2—Thinking About Cross-Domain Deterrence In Phase Zero

This panel focused how two of America's potential rivals, the Russian Federation and People's Republic of China, think about deterrence and coercion in "phase zero," or before crisis begins. It also explored what the United States should do in response.

Russian Cross-Domain Thinking

Since 1999 when NATO used precision guided munitions on a large scale during *Operation Allied Force* in Kosovo, Moscow has dedicated significant intellectual capital to thinking about how it will maintain its security against what it perceived to be a significant security threat given its conventional military decline. Despite the sense of urgency to improve Russia's military capabilities the NATO campaign in Kosovo created, it must be noted that deterrence has always been cross-domain in the Russian experience. Today, Russia has developed a well thought out strategy to integrate its instruments of power to protect itself from a variety of perceived threats.

Open source literature suggests the Russian Federation perceives four main threats to its security: 1) the massive employment of conventional precision-guided munitions, 2) the expansion of a ballistic missile defense system it believes threatens its strategic nuclear deterrent's viability, 3) political uprisings or a "color revolution" in Russia, and 4) the threat of Islamic extremism.

Given these threat perceptions, the Russian Government has devoted significant energy to developing an information warfare strategy that operates in peacetime, during times of escalating crisis, and after conflict begins. This information strategy integrates all relevant government agencies into a "whole-of-government" approach to deterrence and coercion aimed at frustrating and slowing Russia's adversaries' decision-making cycle.

Chinese Cross-Domain Thinking

China's "Three Warfares" information strategy is, according to some seminar participants, a well-developed strategy for deterrence, compellence, and countering U.S. power projection in phase zero. This strategy is comprised of legal, public opinion, and psychological warfare components. Chinese security professionals openly discuss the "Three Warfares" and the People's Liberation Army has the vested authority to implement the strategy.

China's "Three Warfares" and broader international strategy is being used by the PLA and Chinese Government to achieve deterrence by the threat of an unacceptable retaliatory action and to compel states to take actions with favorable results for Chinese interests. This strategy that integrates deterrence and compellence differs from the U.S. experience of thinking about deterrence and compellence as separate, unrelated concepts.

Like Russia, deterrence has always been cross-domain in the Chinese experience and China is focused on demonstrating its current capabilities, future potential, and willingness to employ the tools at its disposal to deter its adversaries. Despite the similarities in China's approach to signaling resolve relative to the U.S. and Russia, panelists discussed how China takes a much different approach to dealing with crisis than the U.S. and Russia. The U.S. and Russia have long treated the processes of escalation and de-escalation in an unfolding crisis as a "third player" in deterrence interactions. In this framework, crises are understood to take on dynamics of their own that can be difficult to control, and thus are also another source for potential miscalculation or unforeseen outcomes. China thinks differently about this, with the premise that conflicts are generated and controlled through deliberate choice and action. This is a significant mismatch of strategic culture with implications for strategic stability.

The opacity of the Chinese decision-making process increases the escalation potential between the U.S. and China in addition to the risk posed by their different view of crisis. It is unknown how exactly and by whom decisions about crisis management would be made in China. For example, eight years after the 2007 Chinese anti-satellite weapon test that created a cloud of space debris in orbit, little is known about how the decision to test that weapon system was made and whether those who made the decision were aware of the test's consequences—begging the question of whether China at that time had integrated and coordinated the relevant agencies involved in strategic space operations.

Panel 3—Managing Escalation Across Domains

This panel focused on managing escalation within the space and cyber domains, where escalation dynamics are less understood than in the traditional air, sea, and land domains.

Each panelist and many of the seminar participants acknowledged that deterring attacks in the space and cyber domains would be especially difficult because of U.S. asymmetrical advantages in these domains. Furthermore, escalation in these domains is unlikely to be predictable because of the dearth of historical examples, a lack of common vocabulary among the U.S. and its adversaries, and the unpredictability inherent to crises.

Potential U.S. Cross-Domain Strategies for Deterrence

Despite the inherent difficulties of deterring space and cyber attacks, five deterrent strategies were proposed, each with various tradeoffs:

1) Counter-force: once a space or cyber asset is attacked, the U.S. would destroy the adversary's counter-space and counter-cyber assets—perhaps pre-emptively. This strategy might be easier to implement for high-end attacks versus low-end attacks, but might pose credibility issues.
2) Counter-value: because the U.S. highly values its space and cyber assets in ways its potential adversaries might not, this strategy would make deterrent threats against the high-value targets of U.S. adversaries in different domains.
3) Symmetrical or "tit-for-tat:" while technically feasible, this strategy may only pay small dividends and has issues with credibility and proportionality due to the reliance on space and cyber systems that America's adversaries do not reciprocate.
4) Denial: this strategy seeks to deny the benefits of an attack on computer or space assets. It relies primarily on enhancing the redundancy and resiliency of these systems.
5) Ambiguity: this strategy highlights the complexity of military action in these domains and stresses that attack on these assets could lead to unpredictable and thus undesirable outcomes.

Cross-Domain Deterrence Challenges

Many of the issues raised with the deterrence strategies discussed above remained unresolved. In the cyber domain, it remains unclear what type of actions and attacks can and should be deterred. One argument posits that only high-impact attacks that compromise the integrity of important information systems should be deterred (e.g. the OPM breach) and low-impact events given a much lower priority (e.g. the recent Ashley Madison hack). It is unclear intra-domain deterrence is possible in the cyber domain. There is no evidence to suggest cyber attacks ensure the same level of restraint on behalf of our adversaries that U.S. precision-guided weapons and other capabilities do.

In the space domain, the questions about the utility of symmetrical responses to space escalation that were introduced above dominated the discussion, but the question of a U.S. incentive to engage in a space first-strike remained unresolved. In contrast to the view U.S. advantages in space might create an adversary incentive to strike first, this advantage might make a U.S. preemptive strike in space to protect U.S. space assets a viable strategy.

Panel 4—Defining A Pathway To Integrated Strategic Warfare

Challenges to U.S. Integration

This panel focused on the barriers to integrated strategic warfare and how those barriers might be mitigated. Of primary concern to the panelists and participants was that the U.S. is not institutionally organized for integration. Military, intelligence, and policy organizations in the strategic community are highly specialized with information flows that travel up and down through their respective hierarchies. The "stovepiped" nature of the agencies and organizations required for strategic operations in the U.S. government hampers the flow of information among the different agencies and organizations, making integration increasingly difficult.

In the discussion concerning the pursuit of U.S. integration, a definitional question arose that was not present in discussions of Chinese and Russian strategic integration: What does integration mean and how would integration manifest itself in the U.S. strategic community? A definition of integration taken from U.S. Special Operations Command was proposed: "The application of resources from multiple sources in a coherent fashion to achieve synergistic effects at times and places of our choosing." To achieve this, not only must the interaction between regional and functional combatant commands in the U.S. military increase, but civilian agencies must be incorporated as well.

Crisis and unprecedented threats have historically been the driving force behind previous U.S. actions that have integrated military and civilian organizations and agencies. The nature of these events ensures they are unexpected, increasing the difficulty of integrating strategic capabilities before an unforeseen crisis develops. Despite the difficulty inherent to integrating capabilities to address new crises and threats, there are steps that can be taken to improve U.S. integrated strategic capabilities.

Improving the Integration of U.S. Capabilities

One method to improve the integration and coordination between disparate military and civilian agencies and organizations is to continue exchanging personnel between different agencies and organizations. The temporary assignment of personnel to different offices with similar mission sets improves relationships and trust between the organizations and their staff. This relationship and trust building can help to mitigate the negative effects of intra-governmental competition for limited resources, which can negatively impacts integration and communication between organizations.

Military tabletop exercises and Title X war games are other avenues to help improve the integration between organizations and the relationships between their staff. These exercises improve the coordination amongst organizations and also help identify potential vulnerabilities. Panelists stressed that these exercises must be made more realistic and should simulate the bureaucratic challenges and uncertainty present in crisis.

The possibility of integrating the various policy and posture reviews conducted periodically by the Department of Defense (e.g. the Quadrennial Defense Review, Nuclear Posture Review, Ballistic Missile Defense Review, etc.) into a comprehensive deterrence review was discussed. This approach could reinforce the desired integration of plans, concepts, and forces while facilitating the needed comprehensive approach to balancing investments and risks. But it may prove easier said than done. Different capabilities have different stakeholders inside and outside the Department of Defense, each with competing priorities and incentive structures.

Conclusion

Given the uncertainty highlighted in each of the panels regarding the utility of the term "cross-domain deterrence," responding to how potential adversaries have organized their cross-domain strategies, managing escalation across domains, and the challenges to integrating U.S. strategic capabilities, there is significant room to improve our understanding of CDD. To this end, LLNL and other institutions across government, academia, and the think tank community have dedicated themselves to developing a research agenda for the coming year to improve the community's understanding of CDD when it meets for the 3rd annual deterrence seminar in 2016.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-TR-682064