2015 Cross-Domain Deterrence Seminar

Bibliography

CGSR
Center for Global Security Research

LLNL-TR-681997

LAWRENCE LIVERMORE NATIONAL LABORATORY

2nd Annual Cross-Domain Deterrence Seminar Bibliography

Seminar convened on 17 November 2015 by the
Center for Global Security Research (CGSR)
National Security Office (NSO)
Global Security Program
Lawrence Livermore National Laboratory

Compiled by Anthony Juarez

In November 2015, the Center for Global Security Research, NSO, and Global Security program jointly sponsored a seminar investigating questions related to cross-domain deterrence at Lawrence Livermore National Laboratory. At the seminar, experts were asked to moderate discussion based on the four topics below. For each of these topics, we have compiled a short list of literature that will help analysts develop a baseline understanding of the issue.

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

A summary report of the seminar may be found at https://cgsr.llnl.gov/content/assets/docs/CDD_Seminar_2015_Report.pdf.

1. Assessing Our Progress In Thinking Cross-Domain

Dawkins, James C., Jr. (12 February 2009). *Rising Dragon: Deterring China in 2035.* Research Report: U.S. Air Force War College. Pp. 12, 49-53. (http://www.au.af.mil/au/awc/awcgate/cst/bh2009_dawkins.pdf).

Brig. Gen. James Dawkins Jr. wrote this research report in 2009 as a Colonel at the Air War College before assuming his current role as Director of Strategic Capabilities Policy for the National Security Council. Dawkins' report is the first in the academic literature to provide a working definition of "cross-domain deterrence" in response to what he views as the importance of cyber, space, and economics to future deterrence architectures against peer-competitors, specifically China. Dawkins outlines the factors that will influence China's deterrence cost-benefit analysis and U.S. strategies for implementing extended deterrence in Northeast Asia.

Denning, Dorothy E. (April 2015). Rethinking the Cyber Domain and Deterrence. *Joint Force Quarterly,* No. 2. (http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_8-15_Denning.pdf)

Dorothy Denning of the Naval Postgraduate School tackles arguments that the man-made nature of the cyber domain and its malleability distinguish it from the other warfighting domains. Instead, she argues that these qualities showcase cyberspace's similarity to traditional domains. This is particularly important since the salience of cross-domain deterrence is widely attributed to the importance of space and cyberspace to military operations. Denning concludes by offering two strategies for deterring attacks in cyberspace.

Frankel, Michael, James Scouras, and George Ullrich. (2015). *The Uncertain Consequences of Nuclear Weapons Use*. Baltimore, MD: Johns Hopkins Applied Physics Laboratory. (http://www.jhuapl.edu/newscenter/publications/pdf/TheUncertainConsequencesofNuclearWeaponsUse.pdf)

How nuclear weapons might fit into a cross-domain deterrence framework (and whether they should be included at all) was a question addressed at the 2015 CDD Seminar. Frankel, Scouras, and Ullrich argue that gaps in the nuclear effects knowledge base will prevent a comprehensive understanding of the effects of nuclear weapons, especially at the low-end. They argue that by filling this gap in the knowledge base of nuclear effects, more viable deterrence architectures and operational plans can be developed.

Gartzke, Erik and Jon Lindsay. (15 July 2014). *Cross-Domain Deterrence: Strategy in an Era of Complexity.* University of California, San Diego. (https://quote.ucsd.edu/deterrence/files/2014/12/EGLindsay_CDDOverview_20140715.pdf)

Gartzke and Lindsay argue that the growing complexity that characterizes the security landscape has become a strategic problem. They outline the deficiencies in U.S. understanding of the potential for escalation, the interpretation of signals, and the effects of operations across the warfighting domains. They conclude by describing a research agenda that will help develop U.S. strategies to better understand cross-domain effects and create cross-domain deterrence architectures.

Lewis, James A. (July 2010). *Cross-Doman Deterrence and Credible Threats.* Washington D.C.: Center for Strategic and International Studies. (http://csis.org/files/publication/100701_Cross_Domain_Deterrence.pdf)

Among the first to write about cross-domain deterrence, James Lewis describes the changing contemporary threat environment and the challenges inherent to developing deterrence architectures addressing these threats. Lewis describes the asymmetry of stake involved in various domains and the implication of this asymmetry—that credible threats to deter action in space or cyberspace cannot be domain limited.

Vince, Robert J. (1 May 2015). *Cross-Domain Deterrence Seminar Summary Notes.* Lawrence Livermore National Laboratory. (http://www.slideshare.net/LivermoreLab/summary-notes-47797997)

This document summarizes the proceedings of the first Cross-Domain Deterrence Seminar at Lawrence Livermore National Laboratory. It serves as a useful baseline for assessing how far the strategic community has come since the first CDD seminar at the end of 2014.

2. Thinking About Cross-Domain Deterrence In Phase Zero

Adamsky, Dmitry (Dima). (November 2015). Cross-Domain Coercion: The Current Russian Art of Strategy. *IFRI Proliferation Papers,* No. 54. (http://www.ifri.org/en/publications/enotes/proliferation-papers/cross-domain-coercion-current-russian-art-strategy)

Adamsky describes the evolution of Russian strategic thought, specifically as it relates to its strategy of coercion and the role of nuclear weapons therein. Adamsky argues three main points: 1) that nuclear weapons cannot be analyzed as a separate component of russian operational art, 2) that Russia's cross-domain coercion campaign integrates nuclear, non-nuclear, and informational tools, and 3) that its coercion campaign involves an holistic cyber campaign.

Cheng, Dean. (11 July 2013). Winning Without Fighting: The Chinese Psychological Warfare Challenge. *Backgrounder No. 2821.* The Heritage Foundation. (http://thf_media.s3.amazonaws.com/2013/pdf/bg2821.pdf)

Dean Cheng outlines the Chinese "Three Warfares" psychological and information warfare strategy (discussed in the 2015 CDD Seminar summary report). The objective of this strategy, he argues, is to psychologically outmaneuver China's adversaries and "win without firing a shot." Cheng provides policy prescriptions for how the U.S. should counter China's strategy.

No Editor. (September 2015). *Information at War: From China's Three Warfares to NATO's Narratives.* Transitions Forum. London, U.K.: Legatum Institute. (https://lif.blob.core.windows.net/lif/docs/default-source/publications/information-at-war-from-china-s-three-warfares-to-nato-s-narratives-pdf.pdf?sfvrsn=2)

This volume highlights the information strategies that China and Russia utilize, namely China's "Three Warfares" and Russia's reflexive control strategies, to influence the actions that their adversaries take. It also contains sections stressing the necessity of a strategic and operational narrative for NATO and a framework for "information defence."

Pomerantsev, Peter and Michael Weiss. (2014). *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money.* New York, NY: The Institute of Modern Russia. (http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf)

Pomerantsev and Weiss describe the Kremlin's information operation toolkit, the weak spots in Western society that Russia is targeting with its information operations, and outline recommendations to counter what they call the Kremlin's "anti-Western Internationale."

Thomas, Timothy. (2015). Russia's Military Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led. *Journal of Slavic Military Studies,* 28. Pp. 445-461. (http://www.tandfonline.com/doi/abs/10.1080/13518046.2015.1061819?journalCode=fslv20)

Timothy Thomas details how components of Russia's military strategy may have been implemented in Ukraine. Specifically, Thomas describes how Putin's personal logic and the General Staff's favor of non-military versus military tools played key roles in the Ukraine crisis.

Thomas, Timothy. (Winter 2014-15). China's Concept of Military Strategy. *Parameters,* 44(4). Pp. 39-48. (http://strategicstudiesinstitute.army.mil/pubs/parameters/Issues/Winter_2014-15/7_ThomasTimothy_ChinasConceptofMilitaryStrategy.pdf)

In contrast to Cheng's 2013 summary of a specific Chinese strategy (its "Three Warfares"), Timothy Thomas describes how China thinks about military strategy more broadly. Thomas' analysis describes how China views strategy more holistically than the U.S. military. He notes that Chinese views of strategy bear characteristics resembling Soviet and Russian "reflexive control" strategies that aim to influence an adversary's actions in a way that suits China's objectives, while convincing the adversary that the actions are in their interest.

3. Managing Escalation Across Domains

Cooley, Brendan and James Scouras. (2015). *A Conventional Flexible Response Strategy for the Western Pacific.* Baltimore, MD: Johns Hopkins Applied Physics Laboratory. (http://www.jhuapl.edu/newscenter/publications/pdf/AConventionalFlexibleResponseStrategyfortheWesternPacific.pdf)

Cooley and Scouras argue that developing a more flexible set of capabilities might help maintain a cooperative relationship with China, while at the same time maintain a deterrent against high and low-end conflict in conjunction with existing Air-Sea Battle capabilities. They propose a new "conventional flexible response" with three components: 1) an anti-access area denial component that prevents Chinese access to the geographic areas it could potentially threaten, 2) a distant blockade option to deter escalation via punishment, and 3) the development of new low-end capabilities to make sure the U.S. can operate in the Western Pacific in contingencies with limited objectives.

Lin, Herbert. (2012). Escalation Dynamics and Conflict Termination in Cyberspace. *Strategic Studies Quarterly,* Fall 2012. (http://www.au.af.mil/au/ssq/2012/fall/lin.pdf)

Herbert Lin defines the basic terminology and concepts of cyber operations before providing analysis on how conflict in cyberspace may start, how it could be deescalated, and how cyber conflict could spill over into other kinetic domains.[1]

[1] For those seeking additional insight into the complexities of how cyber weapons work, see: Kim Detter's *Countdown to Zero Day* (2014), which provides an informative narrative on the Stuxnet cyber weapon.

Manzo, Vincent A. (April 2015). After the First Shots: Managing Escalation in Northeast Asia. *Joint Force Quarterly,* No. 2. (http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_91-100_Manzo.pdf)

Vincent Manzo describes the evolving security environment in Northeast Asia and provides concepts useful in framing analyses about escalation management in a Northeast Asian conflict with China or North Korea.

Manzo, Vincent A. (December 2011). Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyber-Space Fit? *Strategic Forum,* No. 272. (http://digitalndulibrary.ndu.edu/cdm/ref/collection/ndupress/id/45581)

Among the earliest articles on cross-domain deterrence, Manzo's article discusses how space and cyberspace might fit into cross-domain operations, deterrence, and the escalation of conflict. Manzo concludes with a recommendation to develop a shared framework to help assess how U.S. adversaries may view proportionality, deterrence, escalation, and credibility.

Morgan, Forrest, et al. (October 2015). *Confronting Emergent Nuclear-Armed Regional Adversaries: Prospects for Neutralization, Strategies for Escalation Management.* Santa Monica, CA: RAND. (http://www.rand.org/content/dam/rand/pubs/research_reports/RR900/RR974/RAND_RR974.pdf)

Morgan and his coauthors address one of the most complex problems facing the U.S. government: If necessary, how will it manage escalation with nuclear-armed adversaries in regional conflicts? This problem is inherently cross-domain, as the nuclear shadow looms over the use of any type of conventional force that may cross one party's nuclear threshold.

Morgan, Forrest E. (Winter 2012). Dancing With the Bear: Managing Escalation in a Conflict With Russia. *IFRI Proliferation Papers,* 40. (http://www.ifri.org/sites/default/files/atoms/files/pp40morgan.pdf)

In thinking about how to manage escalation in a conflict with Russia, Morgan begins with a review of Cold War-era work on escalation management. Morgan concludes by emphasizing the importance of threshold management and identifying the key interests of states as well as their critical thresholds.

Morgan, Forrest E., et al. (2008). *Dangerous Thresholds: Managing Escalation in the 21st Century.* Santa Monica, CA: RAND. (http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG614.pdf)

This RAND study is the basis for Morgan's work in 2012 on managing escalation with Russia. Unlike his 2012 article, in this article Morgan and his coauthors focus on the challenges of managing escalation in a conflict with China.

4. Defining A Pathway to Integrated Strategic Warfare

Schnaubelt, Christopher M. (ed.). (2011). *Towards a Comprehensive Approach: Integrating Civilian and Military Concepts of Strategy.* Rome: NATO Defense College. (http://www.ndc.nato.int/download/downloads.php?icode=272)

In pursuit of the goal of integrating the various instruments of state power, the authors of this volume have focused on how military and civilian versions of strategy differ and how they can be integrated. Among other topics, the volume investigates historical cases of civil-military integration (or the lack thereof) and the challenges to pursuing a comprehensive approach to warfare.

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-681997