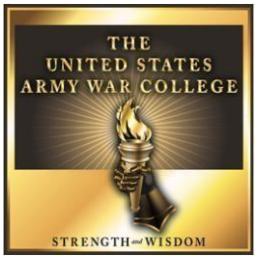
Strategy Research Project

Escalation Dominance in the Information Age

by

Lieutenant Colonel John Mark Wilson
United States Army

Under the Direction of:
Dr. M. Chris Mason



United States Army War College
Class of 2017

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2017	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Escalation Dominance in the Information Age

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel John Mark Wilson
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. M. Chris Mason

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution A: Approved for Public Release. Distribution is Unlimited.

To the best of my knowledge this SRP accurately depicts USG and/or DoD policy & contains no classified information or aggregation of information that poses an operations security risk. **Author:** ☒ **PA:** ☒

13. SUPPLEMENTARY NOTES
Word Count: 5,050

14. ABSTRACT

Many prominent Cold War-era thinkers and practitioners argued that escalation dominance, a condition where a competitor is more willing and capable of discouraging an opponent from taking an unwanted action at all levels of conflict short of nuclear war, is necessary to achieve success in deterrence strategies. The rapid evolution of information systems and networks has connected people and institutions more closely today than during any other point of human history. As such, the contemporary information environment affords weaker states and non-state actors greater opportunities to employ asymmetric stratagems to deny their stronger opponents' deterrence objectives. This project examines escalation dominance theory in the modern context and concludes that the contemporary information environment has reduced its value in predicting deterrence outcomes. Today, weaker nations and non-state actors are using the ambiguity and relative novelty of cyberspace to create opportunities to advance national interests without causing escalations with stronger nation states.

15. SUBJECT TERMS
Deterrence

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	25	

Escalation Dominance in the Information Age

(5,050 words)

Abstract

Many prominent Cold War-era thinkers and practitioners argued that escalation dominance, a condition where a competitor is more willing and capable of discouraging an opponent from taking an unwanted action at all levels of conflict short of nuclear war, is necessary to achieve success in deterrence strategies. The rapid evolution of information systems and networks has connected people and institutions more closely today than during any other point of human history. As such, the contemporary information environment affords weaker states and non-state actors greater opportunities to employ asymmetric stratagems to deny their stronger opponents' deterrence objectives. This project examines escalation dominance theory in the modern context and concludes that the contemporary information environment has reduced its value in predicting deterrence outcomes. Today, weaker nations and non-state actors are using the ambiguity and relative novelty of cyberspace to create opportunities to advance national interests without causing escalations with stronger nation states.

Escalation Dominance in the Information Age

The purpose of this research paper is to examine the escalation dominance concept in the contemporary information environment. This study recognizes the added complexity the information environment imposes upon actors competing in today's international system. As such, it operates from the premise that while visible military capabilities are critical components in determining deterrence outcomes, the skillful application of less visible, non-military instruments of power across domains play an increasingly prominent role in determining deterrence outcomes. By identifying areas where the complexity and ambiguity of the cross-domain security environment are not applicable to the widely-discussed theory of escalation dominance, this study provides policy makers and strategic leaders with a start point for efforts to adapt strategy. The research question is this: How should the contemporary information environment, which includes the cyber domain, change US strategic thinking about escalation dominance? This study concludes that the contemporary information environment has reduced the value of escalation dominance in predicting the outcome of deterrence actions.

The study will answer the research question in five phases. First, the study will establish the definition of "deterrence" used throughout the analysis. Second, the author will survey existing literature on escalation dominance to identify salient themes for analysis. Third, the author will provide a description of the contemporary information environment for future analysis. Fourth, the study will evaluate the applicability of escalation dominance in the contemporary security environment. Fifth, the study will discuss strategic implications and provide recommendations.

Deterrence

The purpose of this section is to establish a definition of "deterrence" used throughout this study. The rise of non-state actors as competitors, Chinese expansionary activities in the South China Sea and Russian aggression in Eastern Europe have regenerated discussion about the efficacy of deterrence in addressing these strategic problems. While defense involves unambiguous, *ex-ante* actions to prevent an enemy's seizing an object, deterrence focuses on less visible, *ex-post* communications aimed at dissuading an opponent from further pursing an undesirable action. Therefore, deterrence involves the communication of overt or tacit threats, promises, and punishments directed at the opponent's decision-making system, based upon the careful measurement of interests and intentions.

A recent NATO study describes deterrence as "the threat of force to discourage an opponent from taking an unwelcome action. This can be achieved through the threat of a retaliation (deterrence by punishment) or by denying the opponent's war aims (deterrence by denial)."[1] Laurne et al. describes five principles of deterrence strategy. First, strategists must carefully evaluate competing national interests to determine if their importance warrants unambiguous defense or a subtler deterrence. Second, the strategy must deliver a clear communication of national commitment. Third, deterrent threats must be credible and sufficient to achieve planned outcomes. Fourth, for threats to be credible, they must be connected to national security. Finally, the denial of the opposition's desires must not result in an immediate act.[2]

The previous description, definition, and principles create a simplistic view of deterrence, belying its complexity. As discussed in the subsequent section, numerous theorists understood the inherent complexity of deterrence and, by extension, the

concept of escalation dominance. A survey of their thinking is an essential step to examining escalation dominance in the contemporary security environment.

Escalation Dominance Literature Survey

The purpose of this section is to draw upon the body of literature related to escalation dominance and to identify salient themes and concepts for analysis. Escalation dominance is a leading concept in deterrence theory literature. Paul Nitze argues that escalation dominance is a condition where a combatant is capable of defeating attacks at all levels of conflict except for the highest, nuclear war. He states, "It is a copybook principle in strategy that, in actual war, advantage tends to go to the side in a better position to raise the stakes by expanding the scope, duration or destructive intensity of the conflict. By the same token, at junctures of high conflict short of war, the side better able to cope with the potential consequences of raising the stakes has the advantage. The other side is the one under greater pressure to scramble for a peaceful way out. To have the advantage at the utmost level of violence helps at every lesser level."[3] Consequently, Nitze argues that in limited warfare scenarios, escalation dominance is not simply a function of the aggregate capability of a state to inflict punishment or damage upon an adversary. Instead, he argues that a state with escalation dominance is better postured to deploy what capability it has relative to its opponent.

Herman Kahn likens deterrence to an *escalation ladder* where both sides engage in conflicts on "rungs" ranging from low-level engagements to nuclear war.[4] States defeated in these conflicts have the option to escalate tensions, return to a lower level of conflict, or return to the pre-hostility status quo. Two ideas are central to this approach. First, Kahn posits that a predictable process of escalation/de-escalation and

the lack of ambiguity in the states' intentions are essential conditions for effective deterrence.[5] Second, Kahn appears to imply that a state's military must visibly demonstrate its capability to defeat its adversaries' forces at all levels of conflict for threats to be credible.[6]

Khan envisions deterrence as a linear process that, by its nature, reduces the risk of escalation. A key assumption underscoring Kahn's thinking is that competing states have a common understanding of one another's thresholds of escalation/de-escalation. As such, strategists working within the escalation dominance framework must calculate the level of military force required to compel a return to the status quo. The risk associated with developing strategy within the escalation dominance framework is miscalculation of the amount of force required, creating the unintended consequence of either showing a lack of resolve or a lack of willingness to engage in a conflict whose cost is too high. Similarly, as Kahn points out, at each "rung" of the escalation ladder, each side of a conflict has a different set of capabilities with which to compete. Per Kahn, the result of this asymmetry of capabilities at a lower level of conflict increases the difficulty for one side to escalate.[7]

Like Kahn, Byman and Waxman highlight asymmetry as a key element in deterrence theory. They observe that "a critical condition of successful coercion is escalation dominance: the ability to increase the threatened costs to the adversary while denying the adversary the opportunity to negate those costs or to counterescalate."[8] They further explain that escalation dominance means that no matter what an adversary does to apply pressure, the coercer is always able to overwhelm the adversary in that specific area. As discussed in greater detail in subsequent sections of this study, the

increased complexity of today's information environment compared to that which existed during the Cold War provides competing parties more conduits and opportunities for the employment of asymmetric deterrence stratagems.

Communications is another salient theme in deterrence theory. While Kahn saw clarity as essential for states seeking to express credible deterrent actions, economist Thomas Schelling held the view that ambiguity was the key. Schelling suggests that states in conflict effectively deter another by coordinating various instruments of power in a subtle manner that leads adversaries to make a best guess that the only way to avoid an undesirable escalation is by maintaining the status quo or deescalating. Such communications are tantamount to a high-pressure bargaining session where the victor is more willing to undertake an undesirable and potentially unintended escalation than its adversary.[9] This does not only include the demonstration of capability, but also the announcing the presence of "thresholds", something a competitor signals to another as an event or phenomena which, should it ever occur, would enlarge conflict.[10]

Schelling describes this subtle form of communications as "tacit" where "communication is by deed rather than by word, and the understandings are not enforceable except by some threat of reciprocity, retaliation, or the breakdown of all restraint."[11] Schelling likened this tacit communication to high-stakes bargaining where an adversary would see the physical actions of another and make new calculations about future actions. Embedded within this analogy are a few key concepts important to analyze in the contemporary environment. First, *trip wires* are stratagems where an opponent places something of value between the adversary and the object it values. As such, the adversary understands that an attack on that trip wire will trigger an immediate

and costly action.[12] For example, the US deployed 12,000 troops as part of the Berlin Brigade to send a strong message to the Soviet Union about its commitment to the defense of West Berlin.[13] Had the Union of Soviet Socialist Republics (USSR) attacked West Berlin, the brigade would have been defeated soundly by an overwhelming force, representing a sunk cost. However, US willingness to absorb this *sunk cost* sent a powerful message to the USSR about the value it placed on the protection of West Berlin.

Another concept related to tacit bargaining is *audience cost*. Fearon observes that the reaction of domestic audiences in competing states is an important factor in measuring willingness to escalate conflict.[14] Additionally, leaders who make threats or promises, but do not follow through on them, lose credibility not just abroad, but also within domestic publics. As such, leaders of democracies are more susceptible to the effects of *audience cost*, complicating the implementation of deterrence strategies. For example, Schelling states that chemical or nuclear weapons were not used in Korea though no formal agreements governing their use existed at the time.[15] As such, he highlights the importance of traditions, understandings, and implied positions in making deterrence decisions. Schelling and Kahn's divergent views of the role of communications in deterrence raises difficult questions about the relationship between the availability of information about intentions and decision-making, particularly in the contemporary age.

The final concept related to tacit communications is *competitions in risk taking*, where an opponent communicates a threat to cross the threshold of a major escalation to meet strategic objectives.[16] Schelling characterizes deterrence as a "threat that

leaves something to chance."[17] Simply stated, Schelling believed both sides of a conflict are subject to risk of escalation, either from accidents or unintended consequences. Both sides are exposed to varying degrees of risk until the conflict is resolved, either through a return to the status quo or escalation into nuclear war. As such, Schelling concludes that deterrence opponents can achieve their goals through the deliberate creation of risk to "[set] afoot an activity that may get out of hand, initiating a process that carries some risk of unintended disaster. The risk is intended, but not the disaster."[18]

A brief description of contrasting characteristics of *competitions in risk* and *escalation ladders* reveal useful insights for understanding the role of escalation deterrence in the modern context. Climbing Kahn's *ladder* primarily involves actions in limited war up until conflict escalates to the point of nuclear war. Limited conflict involves the exchange of pain between combatants, meaning both sides sustain damage. However, with Schelling's *competitions in risk*, a party willing to take an action that exposes it to more risk than simply moving up to the next "rung" forces its more risk-averse opponent to back down and emerges from conflict without having sustained any damage. The *escalation dominance* concepts described are the product of exceptional Cold War-era thinking. In the follow sections, this study seeks to determine the degree to which this thinking remains applicable in the modern security environment.

Key Characteristics of the Contemporary Information Environment

Whereas the development of nuclear weapons gave rise to Cold War deterrence theory, the development of a wide range of information technologies have shaped nature of warfare. As such, it is incumbent among national security thinkers and

practitioners to reconsider the changing nature of deterrence. The rapid expansion of, and evolution of, information systems and networks have resulted in the greatest degree of connectivity between public, military, and private institutions in human history. The evolution of the “Internet of Things,” with everyday devices connected to the network, has further complicated the information environment.[19] Increased connectivity between institutions and people means additional vectors through which actors can conduct cyber intrusions and influence operations, both within and across geographic boundaries.

It follows that if the Information Age has ushered in a new level of complexity for international relations and national security strategy, the same holds true for deterrence. As such, actors seeking to deter adversaries within the international system should seek tools that enhance predictability and control over deterrence outcomes.[20] Therefore, one can conclude that the party most capable of rapidly visualizing threats, trends, and opportunities will have an advantage over its adversary.

Since cyberspace is a salient element of the information environment, strategists and policy makers must understand its implications for deterrence. Near peer competitors such as China have invested significantly into the development of cyberspace capabilities to degrade and disrupt US military capabilities across multiple domains.[21] Access to cyber tools is not limited to nations or even powerful nations. The low cost of entry into the cyber domain makes tools available to smaller nations and non-state actors, as well.

Another key consideration for strategists is attribution. It is difficult to attribute incidents in cyberspace to a specific actor. Though widely suspected of involvement,

reports that Russia used cyberspace tools to support operations during the 2007 Estonia Cyber Attacks,[22] 2008 Russo-Georgian War,[23] and 2014 Russian-Ukrainian Conflict[24] remain officially unconfirmed. The problem of attribution is compounded by the sheer volume of attempted cyber intrusions conducted daily against private, government, and DoD networks. The Pentagon and the National Security Agency (NSA) each sustains approximately 10 million intrusions per day.[25]

The challenge of attribution has two major implications for deterrence. First, not knowing who was responsible for a cyber operation makes target selection for a potential response a high-risk endeavor. Conducting a response against an actor who was not responsible for the cyber operation could result in a loss of credibility and set off new hostilities. Second, as previously discussed, existing theory holds that deterrent threats must be credible and visible. Non-attributable cyberspace operations are often not visible because they draw from a dark network of intelligence agents and cyber operators. Therefore, cyber operations, as a deterrent option, would likely be most effective if used in coordination with other overt instruments of power to demonstrate one's willingness and capacity to use a cyber capability while maintaining plausible deniability. As such, a deterrence competitor integrating cyberspace operations into deterrence stratagems will optimize their employment if the adversary knows it can do it, but is not able to prove attribution.

Another key challenge for strategists is that the cyber domain is largely unknown. Libicki observes that given the complexity of the cyber domain, strategists have little certainty in understanding the potential effects of a cyber attack.[26] Another challenge is linked to the fact that since cyber weapons are rarely used and no case studies

analyzing the use of cyberspace operations during deterrence operations exist, strategists are left to make informed guesses about how the target would respond. Since no historical patterns, norms, or expectations resulting from the widespread employment of cyberspace operations have developed among international actors, planners must make difficult and risky determinations on appropriate deterrence responses to cyber activity. Over such a vast and interconnected network, it is a speculative endeavor to predict with absolute precision how an entire command and control system, from the point of detection to the decision maker, will respond to a cyber attack. Finally, since few laws and policies govern the degree to which private organizations conduct active measures against actors attempting to probe their networks, planners cannot assume that government agencies are alone in conducting responses. This adds an even greater degree of uncertainty about attribution and response to an already inherently complex environment.

This has important implications on how strategists should view cyber operations and deterrence. First, effects of cyberspace operations are likely to be temporary in nature and, at best, will confuse and frustrate opponents. An important characteristic of cyber attacks is that with few exceptions, they do not destroy people or things.[27] Therefore, as previously observed in the discussion on attribution, cyberspace operations are best employed as a supporting instrument to other capabilities. Second, given the amount of work required during operational preparation of the environment (OPE) and the unpredictability of surrounding threats, cyber weapons are best used sparingly and only when the confidence of success is high. Finally, Libicki observes

that, unlike the fear of escalation in the wake of aerial bombing, the targeted adversary will become more resistant to further coercion in the cyber domain.[28]

Analysis

The purpose of this section is to describe key implications which the contemporary security environment has on foundational concepts of escalation dominance. The study first analyzes the related concepts of the escalation ladder and communications. Second, the study will analyze the broader concept of escalation dominance to answer the research question.

Escalation Ladder

The modern environment prompts three major questions for the escalation ladder concept as described by Kahn. The most fundamental question for strategists is understanding when a cyberspace attack is serious enough to warrant a response. During the Cold War, theorists and strategists hypothesized responses and counter-responses based upon widely understood capabilities such as conventional military forces and nuclear weapons. Today, strategists will struggle to predict not only how an adversary will respond to cyberattacks, but also in assessing whether the tacit threat of execution of a cyberspace response would be sufficient to achieve the deterrence objectives.

The nature of this challenge was highlighted in the Obama Administration's plan for cyber deterrence, released in 2015. A key objective expressed in the document was to deter "cyber attacks or other malicious cyber activity intended to cause significant disruption to the normal functioning of U.S. society or government."[29] However, as early as July 2016, US intelligence officials assessed with high confidence that Russia had extracted data from Democratic National Committee networks and conducted intrusions

against state election activities.[30] The fact that the US did not openly develop and communicate a public response until after the national elections speaks to the difficulty of constructing a proportional, appropriate, and timely response to cyberspace activities. Cold War deterrence thinkers did not contend with this specific challenge to the same degree as their successors because they employed more widely understood capabilities. This underscores the need for continued development of planning related to cyberspace.

The second key question which the modern environment raises for the *escalation ladder* model is in understanding where adversaries are operating within spectrum of conflict (e.g., “rung”). While this problem is not specific to the contemporary environment, it is exacerbated by the existence of far greater conduits of information than those existing during the Cold War. This condition increases the probability of system overload, confusion, and slow decision making. Returning to the example of the recent US election, it is likely that both adversaries do not share a common view of where they are operating on the spectrum of conflict. Were the US to view the recent Russian cyber-enabled influence operation against its elections as an independent act, a proportional response might signal US willingness to escalate, prompting the Russians to back down. However, if Russia conducted the influence campaign in response US efforts to foment discontent among the Russian populace after its 2011 presidential elections, a US counter response is likely to result in further escalation.[31] Given the ambiguity, secrecy, and unpredictable nature of cyberspace operations and the volume of information being processed in headquarters today, it is easy to

understand how contemporary decision making systems could suffer from decision making latency.

The final question related to the *escalation ladder* concept in the modern context is related to achieving cross-domain synergy in the contemporary environment. As discussed in the previous section, actions in the cyber and information domains are not likely to achieve the deterrent effect. Contemporary strategists will be required to find ways to group together capabilities across multiple domains to achieve deterrent effects. This is critical to the US right now as many of its adversaries look to create cross-domain synergies to increase their operational reach and flexibility in defeating US deterrence at lower-level “rungs”.

For example, Russia appears to recognize that in the modern security environment, observable instruments of power are not sufficient to achieve national objectives in the limited war context. Therefore, against a stronger opponent such as the US, Russia must asymmetrically employ non-military and less visible instruments. While Russia’s approach is born of conventional military weakness, its power remains fungible because of the mere possibility it could employ non-military means to achieve its ends.[32] This thinking gives Russia an advantage against its stronger opponents whose options are more reliant upon military instruments or do not possess the bureaucratic dexterity to operate rapidly across domains. Consequently, Russia does not view cyber tools as the key to achieving its objectives, but rather its ability to combine cyber activities in concert with other instruments of power. Therefore, an examination of US cyber strategy against Russia should not be limited to tools within

the cyber domain, but rather focus on how the tools interact with other elements of power and the effects they could achieve.

Communications

Second, a key challenge for contemporary deterrence strategists is ensuring the adversary understands it is being threatened or punished. As discussed in the literature survey, effective deterrence is built upon the adversary's knowledge that the action occurred and is linked to the behavior its opponent seeks to deter. This is not to suggest the action must be overt in nature. Non-attributable, low-level actions employed in coordination with other instruments could leave just enough certainty in the adversary's mind about the credibility and source of the threat as to not increase the adversary's audience cost to the point at which an escalation becomes inevitable.

Again, US actions in the wake the Russian influence campaign against the 2016 US presidential election show the relationship between communications and audience costs in the modern information environment. The Russian failure to prevent the compromise of its covert cyberspace and propaganda effort, coupled with heated political rhetoric about the election being "rigged", created significant tension among the US population.[33] This increased US audience cost forced the Obama administration to opt for an overt, public response. While it is too early to assess the effectiveness of these actions in deterring further Russian aggression against US institutions, a key emerging lesson is that contemporary strategists must consider audience cost either in assessing the value of the object they are seeking to protect. Given the increased interconnectivity between public, military, and private institutions in the modern security environment, the likelihood that covert or private communications between actors will not be leaked for public consumption is much lower than during the Cold War era. This

could lead to inescapable escalations. As such, the Information Age has sharpened audience costs for deterrence.

Escalation Dominance

This study concludes that the information age has not rendered escalation dominance an invalid concept when the conflict involves two opposing parties at military parity. Kahn's *escalation ladder* remains a useful tool for strategists and policy makers to visualize how such a conflict would evolve, allowing them to better set conditions for the achievement of escalation dominance. However, Kahn's *escalation ladder* is not as useful today in the context of competitions involving states with mismatched military strength. Weaker states seeking to achieve their objectives would not be keen on trading signals, threats, and punishment with a stronger opponent. While it is possible that weaker states could correctly predict the specific point along the *escalation ladder* where the stronger opponent's computation of cost associated with a major conflict exceeds its benefit, basing a deterrence strategy upon this assumption is a dangerous proposition for weaker opponents. Instead of climbing up and down the escalation ladder, states could create additional rungs invisible to and inaccessible to its stronger opponent.

Tapping into new tools and opportunities in the information environment allows the weaker state to employ asymmetries to defeat deterrence by "readjust[ing] the *status quo* undergirded by deterrence by means of a *gradual alteration of expectations and credibility*."[34] In other words, the weaker party seeks to defeat deterrence slowly and subtly by changing the geopolitical reality in its region. This is particularly relevant when the weaker party is in conflict against an actor who is the beneficiary of extended deterrence provided by a stronger party. For example,

Russian's use of proxies, intelligence operations, and cyber-enabled information warfare (reflexive control) during its 2014 conflict with Ukraine increased confusion about Russian intentions, providing cover for special operations forces operating in Crimea to secure key terrain and link up with anti-Ukrainian irregulars.[35] Additionally, using cyberspace operations, propaganda, political warfare, economic coercion, the agitation of ethnic Russian enclaves, and camouflage to disguise the movement of Russian military equipment into Ukraine, the Russians quietly reestablished the *status quo*, seizing the initiative and forcing the U.S. to recalculate the levels of risk it was willing to accept to deter further Russian aggression against Ukraine.[36]

Another example of this approach to defeating US deterrence strategy involves China's actions in the Pacific. Based upon efforts to normalize Chinese behavior such as the Code of Conduct for Unplanned Encounters at Sea and the use of naval assets to conduct "freedom of passage" operations, US strategy appears to back deterrence with "shaping" diplomacy.[37] Alternatively, China's actions reflect its commitment to strategic asymmetry by employing limited-war techniques to slowly and subtly militarize maritime zones.[38] Like Russian efforts described in the previous paragraph, China shows disregard for US deterrence by using a wide range of national instruments of power to achieve its objectives without pushing conflict over the threshold of a major escalation. Again, the objective is to create a *fait accompli*, forcing the US to operate from a different status quo.

The preceding Russian and Chinese cases share two key characteristics, both presenting problems for US pursuit of escalation dominance. First, both cases involve competitions with state actors operating under US extended deterrence. Second, both

cases involved the extensive, coordinated use of nonlethal and nonmilitary instruments of power below the threshold for escalation to major conflict. Per the phasing construct under which Geographic Combatant Commanders (GCC) operate, most of these activities would occur during Phase 0 (Shape) and Phase 1 (Deter).[39] This highlights a potential vulnerability in the Joint Force's planning systems because in both cases, US deterrence options have not compelled Russia or China to restore the pre-escalation status quo. Instead, Russia and China continue to employ their national instruments of power during periods of "peace" with greater agility than the US.

The question the Joint Force must address, therefore, is whether it is postured to rapidly detect such low-level escalations and act flexibly to counter them without sparking an escalation. Much of the thinking underpinning the Joint Concept for Integrated Campaigning (JCIC) suggests that the Joint Force is postured to achieve Unified Action during Phase II (Seize the Initiative) and Phase III (Dominate), but not during Phases 0 and I.[40] Given the success Russia and China have achieved in defeating US extended deterrence in Ukraine and South China Sea, the Joint Force should reexamine its planning systems to set conditions for better coordination of national instruments of power during steady state operations.

Recommendations

This study concludes that the contemporary information environment has reduced the value of escalation dominance in predicting deterrence outcomes. Near peer competitors are defeating US escalations *ex-ante* by employing a wide range of instruments of national power with great agility to create ambiguity and advance their interests without starting a major conflict. The resultant *fait accompli* renders the US escalation ineffective or too costly because a new geopolitical reality alters the terms of

its deterrence. Recalling Kahn, US competitors are effectively establishing new “rungs” on the escalation ladder without detection by the US. Once the US has determined its adversary has created another “rung,” it must recalculate the deterrence strategy based upon the adversary’s creation of a new geopolitical reality. Under such conditions, US adversaries seize the initiative and dictate the pace of escalation.

As such, strategists and policy makers should consider two recommendations. First, the complexity and volume of the information environment requires the Joint Force to have tools that will allow it to aggregate, index, and visualize developments in the information environment with greater speed. Commonly used in the private sector, these tools can help Geographical Combatant Commands (GCC) identify threats and trends with greater speed relative to the opponent. This will allow GCCs not only to make information-driven decisions with greater speed, but also create a shared view of a complex and ambiguous situation for other Joint Interagency Intergovernmental and Multinational (JIIM) partners. This will also increase the speed of unified action across the services, government agencies, and allied partners, allowing the US to more capably compete with competitors by achieving greater levels of synergy in employing all national instruments of power.

Second, the US should review its posture to conduct effective Phase 0 (Shape) operations. This study highlights the limitations and risks associated with the deployment of additional military capability as a deterrent measure to areas such as the South China Sea, where China is employing asymmetric, non-military measures to achieve its objectives. As the Russian and Chinese cases described in the study show, U.S. moves, often Flexible Deterrence Operations during Phase I, were conducted long

after the adversaries had already constructed a new "rung" or achieved a *fait accompli*. This highlights a need to ensure that GCCs have the tools and authorities necessary to more aggressively counter adversary efforts to seize the initiative and defeat US deterrence during Phase 0.

Finally, the US should examine its own strategic culture as the potential root cause of its failure to deter recent Russian and Chinese aggression. One could argue that the Russians and Chinese view military power not as a distinct competency of strategy, but rather as one of many tools from which to select to achieve political objectives. US doctrine reflects the same core principle. However, US strategic culture and organizational structure differentiate between domains and instruments of power, creating an unwieldy strategic enterprise. This obstacle to the seamless employment of all instruments of national power at all levels of conflict, if not addressed by US policymakers, will enable adversaries to neutralize the potential effect of forward deployed military forces as part of an escalatory package.

Endnotes

[1] Michael Ruhle, "Deterrence: What it Can (and cannot) Do", *NATO Review Magazine*, 2015, http://www.nato.int/docu/review/2015/also-in-2015/deterrence-russia-military/EN/index.htm, (accessed January 27, 2017).

[2] Paul G. Lauren et al., *Force and Statecraft: Diplomatic Efforts of our Time,* 4th ed. (Oxford: Oxford University Press, 2007), 177-180.

[3] Robert Jervis, "The Madness beyond MAD. Current American Nuclear Strategy," *American Political Science Association* 17 (Winter 1984): 34, in JSTOR (accessed January 27, 2017).

[4] Colin S. Gray, "What Rand Hath Wrought," *Foreign Policy* 4 (Autumn 1971): 118, in JSTOR (accessed February 13, 2017).

[5] Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Frederick A. Praeger Publisher), 8.

[6] Ibid., 290.

[7] Kahn, *On Escalation*, 113.

[8] Daniel Byman and Matthew Waxman, "American Foreign Policy and the Limits of Military Might," *Political Science Quarterly* 117 (Autumn 2002): 453, in JSTOR (accessed February 13, 2017).

[9] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 2008),134.

[10] Ibid., 135.

[11] Ibid., 137.

[12] Ibid., 47.

[13] Ibid.

[14] James D. Fearon, "Domestic Political Audiences and the Escalation of International Disuputes," *The American Political Science Review* 88, no. 3 (September 1994): 577, in JSTOR (accessed February 13, 2017).

[15] Ibid., 131.

[16] Ken Watman and Dean A. Wilkening, "Regional Deterrence: The Nuclear Dimension," 1995, http://www.rand.org/pubs/research_briefs/RB24/index1.html (accessed February 13, 2017).

[17] Robert Powell, "Nuclear Brinkmanship, Limited War, and Military Power," April 13, 2014, 17, https://www.princeton.edu/politics/about/file-repository/public/NBMP-140413-Princeton.pdf (accessed February 13, 2017).

[18] Schelling, *Arms and Influence*, 91.

[19] Jacob Morgan, "A Simple Explanation of 'The Internet of Things," *Forbes*, May 13, 2014, http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#61455ef66828 (accessed January 31, 2017).

[20] Jon Lindsay and Erik Gartzke, "Cybersecurity and Cross-Domain Deterrence: The Consequences of Complexity," August 18, 2016, 21, http://deterrence.ucsd.edu/_files/LindsayGartzke_ConsequencesofComplexity_Draft.pdf (accessed February 13, 2017).

[21] Eric Heginbotham et al., "The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power 1966-2017," 2015, https://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR392/RAND_RR392.pdf (accessed February 13, 2017), 260-268.

[22] Sergei A. Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability," 2015, 20, http://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf?sequence=1 (accessed February 13, 2017).

[23] Ibid., 24.

[24] Ibid., 27.

[25] Brian Fung, "How Many Cyberattacks Hit the United States Last Year?" *Nextgov*, March 8, 2014, http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/ (accessed February 13, 2017).

[26] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), xv, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (accessed February 13, 2017).

[27] Ibid., xvi.

[28] Ibid., xv.

[29] The White House, *White House Report on Cyber Deterrence Policy* (Washington, DC: The White House, 2015), http://1yxsm73j7aop3quc9y5ifaw3.wpengine.netdna-cdn.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf (accessed February 13, 2016).

[30] Susan Hennessey, "Is US Cyber Deterrence Strategy More than (Russian) Roulette?" *Lawfare*, blog entry posted October 12, 2016, https://www.lawfareblog.com/us-cyber-deterrence-strategy-more-russian-roulette (accessed February 13, 2017).

[31] David Herszenhorn and Ellen Barry, "Putin Contends Clinton Incited Unrest over Vote," *New York Times Online*, December 8, 2011, http://www.nytimes.com/2011/12/09/world/europe/putin-accuses-clinton-of-instigating-russian-protests.html (accessed January 27, 2017).

[32] Robert J. Art and Kenneth N. Waltz, eds., *The Use of Force: Military Power and International Politics,* 7th ed. (Lanham, MD: Rowman and Littlefield Publishers, 2009), 7.

[33] Hennessey, "Is US Cyber Deterrence Strategy More than (Russian) Roulette?"

[34] A. Wess Mitchell and Jakub Grygiel, "Salami Slicing and Deterrence," *The American Interest*, November 18, 2014, http://www.the-american-interest.com/2014/11/18/salami-slicing-and-deterrence/ (accessed February 13, 2017).

[35] Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," *Understanding War,* September 2015, http://post.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf (accessed February 13, 2017), 17.

[36] Mitchell and Grygiel, "Salami Slicing and Deterrence."

[37] Matthew Hipple, "China: Leap-Frogging U.S. Deterrence in the Pacific," *War on the Rocks,* July 2, 2014, https://warontherocks.com/2014/07/china-leap-frogging-u-s-deterrence-in-the-pacific/ (accessed March 20, 2017).

[38] A. Wess Mitchell, “The Case for Deterrence by Denial,” *The American Interest*, http://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/ (accessed February 13, 2017).

[39] U.S. Joint Chiefs of Staff, *Joint Operational Planning*, Joint Publication 5-0 (Washington, DC: US Joint Chiefs of Staffs, August 11, 2011), III-41.

[40] U.S. Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning* (Washington, DC: U.S. Joint Chiefs of Staff, January 2016), 7, http://www.arcic.army.mil/app_Documents/SLTF/Joint_Concept_for_Integrated_Campaigning_v0_25_14_Jan_2016.pdf (accessed February 13, 2017).