USMA CLASS OF 2006

WAR STUDIES CONFERENCE

REASSESSING DETERRENCE IN THE 21ST CENTURY

13–15 NOVEMBER 2016

War Studies Conference
Reassessing Deterrence in the 21st Century

This is the inaugural War Studies Conference and is sponsored by the Modern War Institute, a research center housed within the Department of Military Instruction at the United States Military Academy, on behalf of the superintendent. The event allows distinguished representatives from the private sector, government, academia, think-tank community, and the joint military services to debate and discuss issues related to modern war and warfare. This year's conference explored the question of whether deterrence, a hallmark of Cold War-era defense policy, is still relevant in an increasingly multipolar world, one increasingly characterized by threats posed by violent non-state actors, hackers, a multitude of small wars, as well as the proliferation of nuclear armed states and our traditional near-peer adversaries like China and Russia. Speakers and participants sought to shed new light on how the United States should modify policy or its military to enhance our deterrence to meet the current threat environment at the tactical as well as strategic level.

Specifically, the conference explored the following:

1) The relevance of deterrence theory, a concept based on rational actors, in today's threat environment of asymmetrical non-state adversaries as well as traditional state actors.
2) How to enhance our 20th-century commitments and alliances (e.g., NATO) to ensure and enhance the robustness of our extended deterrence to our allies.
3) How to rethink the role of deterrence across domains and address challenges posed by emerging issues, including cyberspace, terrorism, and new technologies.
4) How to leverage America's non-military tools of deterrence, including the important role of geo-economics and targeted sanctions, energy, access to financial markets, and soft power.

The above themes will inform a future edited conference volume, coauthored by a select group of participants and other experts, which is intended to frame a conversation with policymakers, senior military leaders, and other decision makers in the years ahead. The War Studies Conference volume will identify specific military implications of changes in the US capacity and credibility to deter our adversaries in the current and future threat environment, as well as make recommendations that follow from these findings.

The format of the conference consisted of four keynote addresses and moderated Q&As, as well as five 90-minute panel sessions with moderators. All panels occurred on a not-for-attribution basis to allow for the free exchange and expression of ideas. Hence, this summary report includes ideas offered during the event, but does not attribute these ideas to specific individuals or organizations. Some of the keynote addresses were on the record at the request of the speaker.

We would like to thank all conference participants for their active involvement and insight in addressing national security reform. A special token of gratitude goes to Maj. Caleb Phillips and Dr. Lionel Beehner, the War Studies Conference Co-Leads. Additionally, the War Studies Conference was made possible under the auspices of the Modern War Institute, and with the support of Mr. Vincent Viola. We are also grateful for the generous support of the USMA Class of 2006, the West Point Association of Graduates, and our media cosponsor, *Foreign Affairs*. Finally, this report is based on notes of the proceedings made by the following rapporteurs, who we would also like to thank: Maj. Mike Jackson, Maj. John Spencer, Maj. Steve Ferenzi, Capt. Nerea Cal, and Mr. John Amble.

LIAM COLLINS, PhD
Colonel, US Army
Director, Modern War Institute
United States Military Academy

Executive Summary

Fifty years after Thomas Schelling wrote *Arms and Influence*, globalization, modernization, and the pervasiveness of non-state actors have fundamentally changed our capacity and our credibility to deter. Deterrence theory tends to be based on Cold War-era state-on-state interactions, as well as on the premises that one could identify the adversary, person or state, that the adversary was a rational actor with highly valued assets one could target, and that if these assets were attacked, it would affect the adversary's decision making, intentions and actions. It also presumed we possessed the means and credibility to threaten these assets. In today's world, however, where adversaries are increasingly networked non-state actors, or lone-wolf actors who carry out cyber-attacks, do these same dynamics and rules apply? If deterrence is "the art of coercion and intimidation," as Schelling noted, how do we coerce non-state adversaries with no return address? How do we intimidate cyber-criminals? How do we keep our 20th-century alliances intact, robust, and capable of extended deterrence going forward? Finally, how can we leverage our geo-economic and other non-military tools of deterrence?

The purpose of this conference was not to hold a dialogue about disarmament or 20th-century concepts like mutually assured destruction. That is, it was not an attempt to put old wine in new bottles. Instead, the purpose was to hold a frank and forward-looking dialogue among a diverse group of thinkers across a broad range of professions to assess whether deterrence is still relevant and the correct lens to think about winning—as well as avoiding—today's and tomorrow's wars. Several key themes emerged from the conference:

- First, the puzzle of the 1950s and 1960s was how to make the threat of escalation into nuclear war credible. While on one hand, that era is over—no region uses nuclear threats to deter or achieve its goals—on the other, intentional nuclear escalation during wartime no longer works as a rational strategy. That is because the seats at the international table have changed: Even though we are the strongest state, small adversaries can still stalemate us.

- Second, information plays a critical role in deterrence, especially in our ability to coerce non-state adversaries: specifically, the ability to understand these actors and the environment in which they are embedded, and how to signal the proper message to induce the desired behavior.

- Third, when it comes to cross-domain deterrence such as cyber, there is an increased need for personal responsibility, defense postures, and information-sharing between governments and the private sector.

- Finally, countries, including near-peer adversaries like China, are increasingly turning to non-military and economic tools to achieve geopolitical ends—a rise in so-called "geo-economics."

This conference hopes to frame the conversation among policymakers and military decision makers on this important topic in the years ahead.

Executive Agenda
13–15 November 2016

Sunday, 13 November 2016

Opening Keynote: "Deterring Revisionist Powers"

Monday, 14 November 2016

Session 1: Revisiting Schelling, Fifty Years On

Motivating Questions

- Is Schelling's concept of deterrence still relevant to today's world?
- If so, how as a concept should it be applied?
- If not, what is the relative theoretical framework for today's and tomorrow's threats?

Session 2: How to Deter Tomorrow's Non-State Adversaries

Motivating Questions

- Are today's non-state actors rational?
- If not, can strategic deterrence work?
- What are some ways to credibly coerce non-state adversaries undeterred by our military "power to hurt"?

Moderated Keynote Q&A Session: "Enhancing Vigilance: Prescriptions for Prevention"

Session 3: How to Fix our 20th-Century Security Alliances

Motivating Questions

- Are 20th-century security alliances still useful for deterrence?
- How does strategic deterrence play in an increasingly multipolar world?
- What are some ways to bolster extended deterrence going forward?

Session 4: Disruption or Deterrence? How to Strengthen US Cyber-Deterrence

Motivating Questions

- How do we successfully deter adversaries in the cyber realm?
- What is the proper role between punishment and denial? Between offense and defense?
- What constitutes an act of war in this domain?

Keynote Address: "Renewing Our Deterrence in Europe"

Tuesday, 15 November 2016

Session 5: Developing Alternative and Non-Military Tools of Coercion

Motivating Questions

- If the power to hurt some of our adversaries militarily no longer holds, what alternative tools should we develop?
- How can we leverage our economic, energy, and soft power assets?
- How should we re-conceptualize cross-domain forms of deterrence?

Closing Keynote and Moderated Q&A: "Big Stick or Soft Power? Domestic Challenges of Deterrence"

Keynote Addresses

Opening Keynote on Sunday, 13 November 2016

Adm. Harry B. Harris, Jr., Commander, PACOM

Moderated Keynote Q&A Session on Monday, 14 November 2016

Mr. Raymond Kelly, K2 Intelligence
Ms. Gayle Tzemach Lemmon, author of *Ashley's War*, Council on Foreign Relations

Dinner Keynote on Monday, 14 November 2016

Gen. (Ret) John P. Abizaid, JPA Partners

Closing Keynote/Moderated Q&A on Tuesday, 15 November 2016

Dr. Eliot Cohen, Johns Hopkins University
Mr. David Sanger, *The New York Times*

Prompt:

The keynote speakers all discussed different theaters where US deterrence is being tested by a variety of adversaries and actors, including at the municipal level, and efforts to deter criminal behavior.

Discussion:

Adm. Harris kicked off the conference by emphasizing the increased importance of the Pacific Command (PACOM) region, especially in terms of economic growth, rapid military buildups and development, and spikes in population. China is expected to eclipse the United States in real GDP growth by the mid-2030s, while its military capability will likely exceed that of the United States during the 2020s. Other fears are that Beijing is trying to rewrite the Bretton Woods regime, which has undergirded the international economic system for the past half-century, with its own free-trade pact, the Regional Economic Program (REPC). To counter the rise of China and deter its aggressive moves in the region, Adm. Harris recommends a four-pronged policy: first, insure the free flow of trade and data in the region; second, reinforce the rules-based international system; third, use diplomacy to bring China into the international system and encourage it to obey international norms; and fourth, enhance our trilateral partnerships with South Korea and Japan. Even if we manage the rise of China, he contends, the greatest threat to regional stability is North Korea and its nuclear development.

Dr. Cohen said that, given the level of interconnectedness of the international system, if the United States were to remove troops from East Asia, then he would expect an increase in proliferation and greater possibility of actual use of these weapons. As such, he argued that it is necessary to maintain our current posture as the global policeman. That is, the military needs to change from its current mindset to what he called "mobilization thinking," specifically given the variety of unpredictable missions it is likely to face. By that, he means a willingness for the military to contemplate unorthodox measures (e.g., direct commissioning) on a scale that DOD is unwilling to consider in peacetime. Moreover, going forward the military should turn to the private sector and tap its national resources, from foreign language speakers to businesses, to meet its mission.

Indeed, Dr. Cohen was less sanguine about the possibility of American soft power to deter but also addressed the domestic political challenges to successful deterrence, one week after a bitter presidential election few would have predicted. "I think it is entirely possible that we are on the verge of some major geopolitical disruption," he said.

Cohen also spoke on the domestic political challenges of deterrence. How does this impact the usefulness of deterrence as a strategic tool in the modern world? "A lot of the intellectual infrastructure of the Cold War, to include the concept of deterrence . . . is a kind of strategic pixie dust," Dr. Cohen argued. "You sprinkle it over a

problem and the problem recedes. And I don't think it's going to work that way [anymore]." This raises the question: If today's domestic political environment means deterrence as we know it is a thing of the past, can it be adapted to apply today's world? And if so, what will it look like?

Another keynote speaker, Gen. (Ret) Abizaid, discussed deterrence in the context of other troublesome regions. He expects the Middle East to remain unstable, particularly in the current environment with Iran's desire to become the champion of Shiites in the region as well as Russia's attempt to reassert its power and influence in the region. Russia has undertaken the actions it has in Ukraine and Crimea because Putin felt he had given too much sway to NATO and by extension, the United States. The key to regional stability, he added, is maintaining the balance of power.

Commissioner Kelly spoke about his long experience with the NYPD, the steps taken to protect New York City against the threat of terrorism after the 9/11 attacks, and his assessment of a range of security threats confronting the United States today. He stressed the need for greater surveillance (e.g., more cameras, undercover informants, etc.), which provided more reliable intelligence and accountability, but also emphasized the importance of greater communication, which comes from having more officers and advisory groups in outer boroughs and Muslim communities.

Panel Session 1: Revisiting Schelling, Fifty Years On

Motivating Questions:

- Is Thomas Schelling's concept of deterrence still relevant to today's world?
- If so, how as a concept should it be applied?
- If not, what is the relative theoretical framework for today's and tomorrow's threats?

Prompt:

This panel featured a number of prominent international relations theorists who were asked revisit themes introduced by the game theorist Thomas Schelling in his seminal 1966 book, *Arms and Influence*. The panel highlighted a few takeaway themes of how to bring deterrence into the 21st century and merge theory onto practice.

Discussion:

According to the panel, the basic elements of coercion are to compel (that is, to force an actor to reverse an action already taken) and/or deter (prevent an actor from taking an action in the first place). But in today's increasingly complex world, compellence is harder. That is because to compel successfully, there must be both threats and deterrence. The trouble is the United States is in the business of deterrence. If the target knows the United States is not going to harm them, neither compellence nor deterrence works. So what determines the credibility of one's threats? Three items: capabilities, resolve, and signaling. On the latter, how does the United States signal to others that we mean business? The problem is that our power undermines signaling—that is, the United States doesn't need to signal if we can strike anywhere in the world in 18 hours. But *not* signaling undermines coercion. So then what determines our credibility? Power is obviously key, but if your resolve is zero, it doesn't work. The United States has power, but it lacks resolve. That is because the determinants of resolve make the United States less credible. During the Cold War, resolve came from ideology, namely anti-communism. But in today's world there is no central ideology, which makes it harder to establish resolve. Back then, moreover, we also had the Domino Theory: That is, we had to fight in Vietnam to deter, say, China. That theory may be long dead but it has been asked: "Who wants to fight for Latvia?" Our commitments today feel less connected and less credible.

Second, the panel posed some questions Schelling did not address that policymakers should focus on: First, how do we extend the framework of deterrence into the acquisition of capabilities? Second, how does our power translate into deterring others from acquiring similar powers and capabilities (i.e., nuclear proliferation)? How should we think of deterrence both pre- and post-conflict. That is, how does one deter the reemergence of violence, which itself is a form of deterrence? Some preliminary answers: international institutions must have the ability to convey information to deter others. If you can develop a nuclear capability without being caught, there is little to deter you; but if you are a part of an international regime, you are more likely to be caught and deterred. For example, the United States deterred Iranian nuclear acquisitions via informational tools that made it known what nuclear capabilities it had.

Third, the panel addressed the subject of terrorism, another subject Schelling did not address except in passing. There is a temptation to overstate the threat posed by terrorists. Moreover, some members of the panel cautioned against treating the absence or occurrence of a terrorist attack as proof that either deterrence worked or failed to work. Deterrence, after all, is about intentions, not estimates. On estimates, the grand mistake of the Cold War was the "desperate intent" to boost our military capacity. But in this case, capacity equals intent. It's easy to mistake the absence of nuclear war for successful deterrence. In fact, Russia did not want World War III, so there was nothing to deter. Flash-forward to the global war on terrorism, where desperate intent infers apparent intent. Policymakers infer that terrorists are good at box cutters, so thus they are probably good at nuclear strikes and we think an attack is imminent, a hypothesis that has guided our post-9/11 strategy. We are told that terrorists can strike anytime and anywhere. While al-Qaeda has signaled its intentions—in 2003, for example, the group said it wanted to strike Saudi Arabia, Sudan, the United States, Britain, Spain, etc.—the group is "a fringe group of a

fringe group," as one panelist put it, lacking in the sophistication or threat matrix we accord them. Richard Reid, the shoe bomber, for example, had a year of training and still could not ignite his bomb. Six Americans die per year from Islamic terrorists—a fraction of the total Americans killed by deer per year. So the question becomes: Are the security measures responsible for these low numbers? Arguably, no.

Fourth, the problems of Schelling's 1950s and 1960s have not gone away. A core pillar of NATO strategy is its willingness to escalate to nuclear warfare as a way to deter or coerce. Russia's strategy is to escalate in order to de-escalate. North Korea's leadership—at least based on their reasonable-sounding pronouncements—has read their Schelling and "flexible response." The problem for military planners is that around the world they are seeking two potentially contradictory objectives: first, to rapidly defeat the enemy; but secondly, not to push the enemy so far that they are so desperate they rely on nuclear deterrence. The end state on the Korean peninsula is in fact the destruction of the DPRK government. In other words, an end state like this one is escalatory by design. In parts of the world where we constrain our end states because they are inherently escalatory, the United States achieves a one-sided success: we have a strategy to avoid fighting a conventional war, but the problem is if we hope to achieve our end state, this is self-defeating. Given the nature of conventional war, which is inherently difficult to control or predict, actions we take in other theaters signal that we want regime change (e.g., DPRK)—and so adversaries reach for the nuclear option as fast as we did in the Cold War to protect their existence. In other words, we inadvertently encourage states to pursue nuclear weapons, not deter them. This is simple game theory: In an analysis of strategic incentives, the same facts that incentivize us are also driving our adversaries.

Panel Session 2: How to Deter Tomorrow's Non-State Adversaries

Motivating Questions:

- Are today's non-state actors rational?
- If not, can strategic deterrence work?
- What are some ways to credibly coerce non-state adversaries undeterred by our military "power to hurt"?

Prompt:

This panel of distinguished academics and defense analysts addressed the enduring dilemma of how to deter non-state adversaries. In today's world, where adversaries are increasingly networked non-state actors or engaged entirely in the cyber domain, do the same dynamics and rules of strategic deterrence apply? How can states deter an enemy that doesn't have a return address? As the 21st-century operating environment increasingly becomes defined by "gray-zone" actors that seek to remain below the threshold of conventional military responses, now more than ever this question demands attention.

Discussion:

Panelists highlighted the critical role of information in deterrence: the ability to understand the adversary and the environment in which it is embedded, and how to signal the proper message to induce the desired behavior. Obtaining such information becomes even more difficult when dealing with non-state actors. Will traditional tools of deterrence work against non-state actors? One member of the panel described how the ability to deter is a function of whether the non-state actor is a proxy of a state—the closer the relationship, the greater the ability to deter. Certain factors influence the likelihood of success: the web of alliances that characterize the relationship; the degree of goal alignment between the sponsor and proxy; and the proxy's organizational structure, capabilities, and breadth of interests. Deterrence is more likely when the non-state actor is allied with a state with whose interests its own are aligned, when it maintains a hierarchical structure, and when its interests are parochial or limited in nature. On the other hand, deterring groups such as the Islamic State (IS) is unlikely. A state may be able to deter individuals from joining or funding the organization, but deterring the group itself, which holds maximalist goals and doesn't answer to a state sponsor, may be impossible. Another member of the panel claimed we are experiencing the "revenge of proxy warfare"—not the Cold War style characterized by favorable leverage asymmetries between sponsor and proxy, but rather one defined by parity. This has policy implications for how much leverage we can actually apply on the state sponsor to deter the non-state actor that doesn't want to comply.

The panel also focused on flaws in conventional wisdom regarding non-state actors. With the traditional focus on terrorism, many scholars take a binary approach because states and non-state actors are viewed as just too different (either no, they cannot be deterred; or yes, but only at the tactical level). One panelist asserted to the contrary that more symmetry exists than previously thought. We must look at the evolution of non-state actors today and revise our assumptions. The military advancement of non-state actors demonstrates a *hybridization* of conventional and irregular capabilities. Their focus on *territorial governance* imposes a different thought calculus beyond simple armed struggle, and their diffusion of power both regionally and locally makes non-state actors today look more "state-like" than often acknowledged.

At the subnational level, Western approaches are handicapped by an excessive focus on "good governance"—creating institutions, rule of law, and public service provision as the antidote for insurgency. In reality, state-building is fundamentally about competition management, and in weak states such as Afghanistan, this means managing the apportionment of power. What we call "corruption" or "neo-patrimonial politics" should be viewed as "preemptive counterinsurgency"—*co-opting spoilers* in order to *deter* them from collapsing the entire state-building project. Would appointing Taliban officials early on have blunted the Afghan insurgency that continues to rage today? This is not the ideal solution from a Western perspective, but rather a suboptimal (but more feasible) course of action that may actually create more stability in the long run. We must recognize that the

interests of the Afghan government are different than ours, and any attempt to work "by, with, and through" a partner nation in a similar context must take this sober reality into account.

Another panelist questioned the actual definition of deterrence. Does it mean maintaining the status quo, preventing escalation, or winning at a low cost? In a tradeoff between winning a military contest and conveying interests without resorting to force, transparency is an essential ingredient. The efficacy of a nuclear deterrent is based on transparency, but tools such as cyber warfare depend on secrecy and deception. Achieving "cross-domain" deterrence in the gray zone requires compromise—utilize low-intensity conflict to maximize efficiency.

Despite the unconventional, and sometimes provocative, nature of the panelists' talking points, questions from the audience focused on the classic issues of leadership decapitation and addressing root causes. Do drones and special operations forces (SOF)-led leadership decapitation work as deterrence? One panelist observed that the use of drones shows that the United States doesn't "really care" due to the low human cost—unmanned aerial vehicles (UAVs) signal low resolve because we are unwilling to put skin in the game. Another commented on the boosting effect for recruitment due to collateral civilian casualties. However, the classification of the drone program makes definitive research difficult. One panelist suggested that more transparency is better, and that the normative costs of civilian casualties may signal resolve that is lost through automation. Drones can degrade and disrupt non-state actors in conjunction with other tools, but they only attack the outputs of insurgency and terrorism, not the underlying grievances.

So then how does one address grievances in order to deter radicalization? A member of the panel emphasized the need to gather micro data at the local level in areas susceptible to extremist influence. What prevents radicalization in the West Bank may differ drastically from what is effective in Yemen. A general policy response for countering violent extremism is not effective. Another panelist agreed emphatically—policy must be supported by research to understand the micro-dynamics and politics on the ground, or else external intervention disrupts the organic processes occurring on the ground and distorts the measures of effectiveness. We need humility about our consistent inability to understand these complex environments.

The themes of discussion throughout this panel highlighted the importance of one underlying ingredient for deterring America's non-state adversaries in the 21st century: informational dominance. To deter non-state actors that serve as state-sponsored proxies, understanding both the adversaries themselves and their patron–client relationship determines where to apply leverage most effectively. When confronting non-state actors via US-sponsored proxies, it is not just a matter of understanding that a difference of interests may exist, but gaining the understanding necessary to identify the appropriate client and then managing such a relationship. For non-state actors not tied to a state, the further down the structures of organizations like al-Qaeda and the Islamic State you go, the more likely you can deter, co-opt, and compel individuals or sub-groups. The question remains: how do you actually identify these elements and induce them to cooperate? This panel provided valuable insight into the viability of traditional tools of deterrence against non-state actors. Reassessing the assumptions that underpin current national security approaches may allow the United States to sharpen its existing tools and develop new ones to confront its non-state adversaries.

Panel Session 3: How to Fix our 20th-Century Security Alliances

Motivating Questions:

- Are 20th-century security alliances still useful for deterrence?
- How does strategic deterrence play in an increasingly multipolar world?
- What are some ways to bolster extended deterrence going forward?

Prompt:

An important element of deterrence is the credibility of collective defense and our "extended deterrence" going forward. The current system of alliances was forged during a different era and under a different international balance of power—before the rise of China, fall of Russia, and resurgence of revisionist states like North Korea and Iran. A hotly debated issue within American military and political circles is whether the United States is getting the requisite bang for its buck with these 20th-century alliances, not to mention that everyone from former Defense Secretary Robert Gates to President-elect Donald Trump have called upon our alliance partners to meet their commitment. This panel addressed the "free-riding" issues inherent in collective security and external balancing as well as how to revamp our extended deterrence in an era of unclear threats.

Discussion:

The panel began with a discussion on the utility of using small troop deployments as "tripwires," which if crossed would trigger a greater commitment of forces and thus deter aggressive behavior. For this approach to be effective, it was argued that US signals and threats will be most effective if they are costly to the United States. Put simply, recent announcements of US and NATO troop deployments in eastern Europe are not costly enough to influence Russia. This is partially because the tripwires are not backed with the risk of nuclear war—the Cold War concept does not translate to eastern Europe today. This leads to two approaches that could work: a much more costly commitment (like what exists in Korea), or for the United States to stop laying tripwires we are unwilling to back up with force.

To address the potential effectiveness of a more costly and larger commitment, the panel provided analysis on both the political relevancy and military efficacy of a war in eastern Europe against Russia. Military war games and simulations have continually demonstrated that the United States never has a clear understanding of Russia's intentions. The war games often speculate that Russia would make a full rush for Baltic capitals, but the strategic or political value of that approach to Russia is not clear, even though the simulations indicate that NATO forces could not stop them. The physical constraints of the Baltic geography and infrastructure make it difficult to defend. Even if NATO wanted to massively increase its military presence in the Baltics, the physical terrain and infrastructure does not allow for enough forces to solve the tactical problem of a concentrated conventional Russian assault into the region or address the likely introduction of irregular, hybrid, or proxy warfare. Thus, it was asserted that any attempt at winning a conventional war in eastern Europe will be costly, ineffective, and likely to escalate. This means that deterrence by denial—or making it almost impossible or prohibitively costly for the adversary to achieve their objective by controlling important terrain with conventional forces—is not a viable strategy in the Baltics.

It's also important to note that assurance and reassurance are complementary to deterrence, but are not the same thing. We confuse those concepts for political motivation. That is, Russia may not want the Baltics, in which case we are not really deterring anything. The Baltic States are not inherently important to the United States; they are only significant within the construct of NATO. This gives Russia the advantage of challenging NATO's credibility through limited expansion—the salami-slicing approach of incremental land grabs that may never trigger full war or a nuclear response from the United States. This leads to a dilemma for the United States: Deterrence by denial may not be possible and with deterrence by punishment it will be difficult to signal credibility against limited, but effective, aggression.

Continuing the discussion, it was emphasized that the United States cannot have a one-size-fits-all deterrence strategy. While we have claimed tailored nuclear deterrence approaches in the past, they were never fully developed. This is particularly important now because nuclear multipolarity changes the model of the bipolar Cold War. Russia has openly articulated an "escalate to de-escalate approach"—defined loosely as using low-yield nuclear weapons as a means to terminate a conventional conflict on terms favorable to Russia—in which we may have to consider, for example, if we would we risk nuclear attacks on the United States to protect Estonia. Given this approach, a limited nuclear response is more appropriate (not mutually assured destruction) and may be a plausible deterrent strategy against Russian aggression. However, since China has a lean and effective nuclear policy with a no-first-strike clause, the threat of a large-scale retaliation may be effective. On yet another hand, it may be more effective to adopt a preemption strategy with North Korea, approaching the regime in Pyongyang as a peer with a damage-limitation option.

Finally, the panel offered insights on the Russian perspective. As one Russian general noted on brinkmanship: "For decades we've stood on the precipice. Today we take a step forward." Though the Americans and Russians have greater frankness and openness with one another than in the past, this understanding does not necessarily bring us closer to them. Moreover, this creates challenges because we now lack mechanisms to de-escalate, a contrast from the Cold War when, for example, Russia shot down approximately 39 US planes, but neither side wanted that known and neither let it escalate into a broader conflict. One panel participant posed the question whether that would or could happen in today's climate.

Two themes arose during the question-and-answer segment: What a Trump administration means for NATO and Russia, and whether there were other non-military options for deterrence that could be more effective. While words matter and hinting at a lesser commitment to NATO can degrade credibility, abandonment is actually more of a possibility in Asia-Pacific than in Europe. It is likely that the Trump administration will walk back some of his campaign rhetoric, especially if NATO members increase their defense spending or make other concessions demonstrating their commitment. What's more, America and Europe's non-military options for deterrence, in some ways, can be constrained by NATO; currently NATO dominates the discussion, but maybe it should not.

Panel Session 4: Disruption or Deterrence? How to Strengthen US Cyber-Deterrence Capabilities

Motivating Questions:

- How do we successfully deter adversaries in the cyber realm?
- What is the proper role between punishment and denial?
- Between offense and defense? Between disruption and deterrence?

Prompt:

This panel featured distinguished panelists representing academia, the military, and the private sector. The motivating questions for the panel address the unique challenges cyberspace poses with respect to the concept of deterrence, including the demonstration of capabilities and difficulty of attributing responsibility; how to define and identify our adversaries in cyberspace; and what role the government, defense, and private actors should take in defending this domain. In this new fluid domain in which the capacity to inflict harm is not constrained to state actors, how can states develop a successful deterrent policy while maintaining an open and global internet? How can government, military, and private industry cooperate to develop effective policies, build capabilities, and train personnel to address this evolving challenge?

Discussion:

Panelists highlighted the tension that results between the United States and our adversaries from differing conceptions of cyberspace. Though the United States hopes to shape a rules-based international order in cyberspace, it has not yet determined how to either *deter* or *compel* action in this new domain. Part of the challenge to effectively deter in cyberspace stems from the difficulty of being able to accurately attribute cyber-attacks. Our adversaries take advantage of the anonymity this domain offers to challenge the United States and its interests. To underscore this point, a panelist described the typical cyber attacker as a "Russian soldier wearing a North Korean uniform, carrying a Chinese weapon and using an Iranian playbook." The ability to mask and obfuscate one's identity in cyberspace complicates how and against whom states should defend and respond.

By deconstructing the concept of deception as it applies to cyberspace, one of the panelists noted that attackers don't always conceal their identities. "Though all cyber operations must be clandestine in order to be successful," as one panelist acknowledged, "they need not be covert." Citing examples like the Free Syrian Army and the United States' development of "loud cyber tools," the panelist urged policymakers to think of attribution not simply as a military problem, but a political one. That is, how does claiming credit either align or undermine a group's political goals and how might a deterrent policy be designed in light of this?

Shifting towards a discussion of how to develop solutions to these problems, the panelists called for an increased emphasis on personal responsibility, defense postures, and information sharing between government and the private sector. Though these approaches seem intuitive, the panelists acknowledged the tension often inherent between public and private interests, especially with respect to privacy, that impedes these partnerships. One participant advocated for a whole-of-government approach in which authorities are aligned with intent, roles and responsibilities are clearly delineated, and capabilities are developed in accordance with these guidelines.

The panelists differed as to whether cyberspace could be understood using existing conventions or if it necessitated the development of new concepts. While most agreed that some concepts still apply (those of secrecy, for example), they acknowledged that the vernacular seems to fall short in practice. Given the speed with which attackers can effect results, the anonymity afforded them, and the constantly evolving methods used, all panelists acknowledged the difficulty in drawing a direct parallel from traditional concepts of deterrence. They discussed the variety of models—including those of disease prevention and economics—being proposed for how to refine the concept of deterrence in cyberspace. This discussion underscored the ongoing debate in the state of the field regarding this issue.

A significant number of the questions raised were related to the role of the military and its realm of responsibility in cyberspace. Most panelists agreed that the military should play a role in protecting critical infrastructure, but disagreed on how to determine which systems are the most critical. For example, while the electrical grid obviously falls into the category of critical infrastructure, the e-mail servers of a private entertainment company may not. Nevertheless, taking into account the cyber attackers' goals and intent and the impact of the cyber-attack, there may be a situation in which this target can be classified as part of our country's critical infrastructure. Beyond *what* the military should be defending, the panelists also discussed *how* it should do so, describing ongoing efforts to build capacity and attract human capital towards this issue. The United States Military Academy's Superintendent, Lt. Gen. Robert Caslen, outlined the programs and initiatives at West Point to educate and train future officers in the skills and aptitudes necessary to successfully operate in this domain. Given the shortage of qualified individuals available in this realm, the panelists also touched on the need to develop public and private education initiatives to fill the gap.

This discussion around the lack of appropriately skilled personnel to counter the current cyber threat prompted a question about whether the military should be training units that don't rely on networks. If our dependency presents such a vulnerability, the audience member queried, shouldn't we create and train units that can avoid that problem altogether? While the panelists found this line of logic compelling, they all seemed to agree that while the concept of mission command allows for operation without networks, it isn't practical in today's operating environment. Instead, the military needs to prioritize which functions are most critical and focus defensive efforts on the systems that fulfill those needs.

The themes of discussion throughout this panel highlighted the criticality of this issue. In an increasingly networked world in which the interests of private citizens, government entities, and private industry overlap and interweave, the application of a traditional conception of deterrence merits significant study and evaluation. Whether with respect to questions of theory, law, technological capabilities, talent management, or training and doctrine, the challenges of cyberspace are some of the most complex, challenging, and important we face in today's operating environment.

Panel Session 5: Developing Alternative and Non-Military Tools of Coercion

Motivating Questions:

- Given the limitations of the military to deter, what alternative tools should we develop?
- How can we leverage our economic, energy, and soft power assets?
- How should we re-conceptualize cross-domain forms of deterrence?

Prompt:

Coercion, we know, does not rest on our military power alone but also includes our soft power, economic might, and other cross-domain sources of leverage. From energy to information, the weaponization of non-military tools has become a persistent feature of the modern battlespace. This panel critically assessed alternative tools of deterrence and how they should be used effectively either as a substitute or complement to military force. In a world of more global peer competitors, how can we leverage our geo-economic strength and statecraft to coerce both adversaries and allies alike? What are the chief impediments—domestic, political, budgetary—to our ability to issue credible threats? Finally, what are some ways we can re-conceptualize cross-domain tools of deterrence? Assuming the 21st-century battlefield will be less conventional or land-based, this panel identified key gaps and vulnerabilities in our arsenal of tools to compel and deter, and pointed out which areas—from energy security to financial tax shelters—we should develop, how to improve civil-military relations in this sphere, and how to enhance strategic deterrence in an increasingly complex and multipolar world.

Discussion:

A few key points emerged from this panel: First, when it comes to deterrence, it's useful to think in terms of a spectrum, with brute force on one end and coercion on the other end. Coercion is much harder now than it was during the Cold War because we used to have one target, and all intelligence collection was focused against it. Now we need universal coverage to understand targets in order to exploit vulnerabilities for coercion. In essence, we still like brute force. Special Operations Forces (SOF) have a role in deterrence, although one member of the panel claimed that SOF capabilities have deteriorated over the past 15 years. When choosing which tools of deterrence to use, often the military is selected because it has a natural constituency that other tools (like, say, the Department of State) lack. SOF needs to be special. Instead, too often we see them as a smaller conventional force that we're willing to deploy and expose to risk in ways we aren't with conventional forces. Thus, the problem is not with the military per se, but with the civilian policymakers. That is, it is politically expedient to "just send some SOF guys," but that is not a clear, focused, or sustainable strategy.

Second, we should not understate the importance of sanctions, deterrence, and war. After all, a strong case can be made that sanctions (namely, against oil) contributed to the start of World War II. To be sure, sanctions today are very different than they were in the 20th century. For one, they are now all about banks. Second, there are three main sanctioning authorities: US, EU, and UN (US OFAC is viewed as the global leader). Third, there are four basic types of sanctions: country-based; list-based (i.e., regime); conduct-based (i.e., non-governments, proliferators, traffickers, terrorists, etc.); and sectoral (these are very complicated). Sanctions are not without complications. A chief concern is the sheer number of parties involved. Another is the difficulty of removing sanctions after a target complies (e.g., Banco Delta Asia and North Korean money; lifting sanctions on Iran, in part because parts of IRGC are still sanctioned). Another problem is the risk of overreach: For example, the United States uses access to New York financial markets as a key coercive tool, which lends it considerable sanctioning power. Today's sanctions are also exceedingly complex. A case in point is Russia, where current sanctions are complicated because they try to thread a needle by limiting reverberations outside Russia but still having a real impact. Finally, when it comes to terrorism, the US Department of the Treasury has realized in the fight against al-Qaeda that informal means are being used (like hawalas). There is a danger when sanctions take away regulated services and push populations toward unregulated services. Another risk comes into play when sanctions empower local actors (e.g., Iran), at the expense of US influence.

Third, whoever controls transportation routes wields leverage in times of conflict. Russia provides another useful example here, with respect to energy routes. First, consider that the EU imports around 15 percent of its gas from Russia. The US approach is based on the core belief that Russian gas exports to Europe can upset European security. Washington has encouraged European partners to seek energy from alternative sources (although US policymakers understand gas from other sources can't really replace Russian gas). There are three principles necessary for US policy to be effective: consistency; responsiveness—that is, the United States must try to find ways to help European partners; and reliability. Without effective US policy—if the United States does not act in a way that reassures European governments—there exists some possibility that Europe will consider seriously the possibility of a European-only version of NATO.

Fourth and finally, countries are increasingly turning to economic tools to achieve geopolitical ends—a rise in so-called "geo-economics." China is doing this well, and Russia has also undertaken geo-economic strategies: Thirty percent of Russia's sovereign wealth fund was used to bail out former Ukrainian President Viktor Yanukovych. More and more countries are turning first to economic tools. What's striking is how many conversations are going on in Washington about deterrence, and yet, consistently, there's no real mention of how the United States should use non-military tools, with the exception of sanctions. Moreover, the United States used to be good at this—influencing events without requiring the use of military power. Our early days as a nation, when Thomas Jefferson was president, provide many examples of this. We also did it well, for the most part, during the interwar period. But from the 1980s, free marketers shaped a view that economics weren't tools and had no role in geopolitics.

Participant List

Name	Affiliation	Role
Gen. (Ret) John P. Abizaid	JPA Partners	Keynote
Dr. Omar Bashir	Financial Integrity Network	Panelist
Ms. Elmira Bayrasli	Foreign Policy Interrupted	Participant
Dr. Lionel Beehner	Modern War Institute	Participant
Mr. Kenneth Bell	Raytheon	Panelist
Dr. Benedetta Berti	TED	Panelist
Dr. Ryan Burke	United States Air Force Academy	Participant
Dr. Risa Brooks	Marquette University	Participant
Mr. Kevin Carroll	Babel Street	Participant
Lt. Gen. Robert L. Caslen, Jr.	United States Military Academy	Participant
Maj. Matt Cavanaugh	Modern War Institute	Participant
Dr. Dianne Pfundstein Chamberlain	Columbia University	Panelist
Dr. Eliot Cohen	Johns Hopkins University	Keynote
Col. Liam Collins	Modern War Institute	Participant
Mr. Yochi Dreazen	Vox	Moderator
Maj. Nathan Finney	The Strategy Bridge	Participant
Dr. Karen Greenberg	Fordham University School of Law	Participant
Dr. Jairus Victor Grove	University of Hawaii at Manao	Panelist
Adm. Harry B. Harris	United States Pacific Command (PACOM)	Keynote
Ms. Jennifer Harris	Council on Foreign Relations	Panelist
Lt. Gen. (Ret) Rhett Hernandez	Army Cyber Institute	Panelist

Dr. Scott Helfstein	Combating Terrorism Center	Participant
Brig. Gen. Diana Holland	United States Military Academy	Participant
Dr. Michael Hunzeker	George Mason University	Participant
Gen. (Ret) Charles H. Jacoby, Jr.	Modern War Institute	Participant
Brig. Gen. Cindy R. Jebb	United States Military Academy	Participant
Dr. Seth G. Jones	RAND	Panelist
Dr. Emmanuel Karagiannis	Kings College London	Panelist
Dr. Nori Katagiri	Saint Louis University	Participant
Mr. Raymond Kelly	K2 Intelligence	Keynote
Mr. Michael Kofman	Kennan Institute	Panelist
Dr. Nina A. Kollars	Franklin & Marshall College	Moderator
Dr. Margaret E. Kosal	Georgia Institute of Technology	Participant
Dr. Matthew Kroenig	Georgetown University	Panelist
Ms. Gayle Tzemach Lemmon	Council on Foreign Relations	Moderator
Dr. Jon R. Lindsay	University of Toronto	Panelist
Dr. Nuno P. Monteiro	Yale University	Panelist
Dr. John Mueller	Ohio State University	Panelist
Dr. T. Negeen Pegahi	Naval War College	Panelist
Dr. Michael Poznansky	University of Pittsburgh	Panelist
Dr. Daryl G. Press	Dartmouth College	Panelist
Lt. Col. Douglas A. Pryer	Joint Chiefs of Staff	Participant
Ms. Alex Quade	War reporter	Moderator
Mr. Stuart Reid	*Foreign Affairs*	Moderator
Lt. Col. Aaron Ressler	United States Air Force Academy	Participant

Brig. Gen. (Ret) Kevin Ryan	Harvard University	Panelist
Mr. David E. Sanger	*The New York Times*	Moderator
Dr. Todd Sechser	University of Virginia	Panelist
Dr. Adam Segal	Council on Foreign Relations	Panelist
Mr. Nicholas Thompson	*The New Yorker*	Moderator
Mr. Vincent Viola	Virtu Financial	Participant