A NEW LOOK AT THE 21ST CENTURY CROSS-DOMAIN DETERRENCE INITIATIVE

SUMMARY OF A WORKSHOP, MAY 19-20, 2016
AT THE GEORGE WASHINGTON UNIVERSITY

Organized by the University Of California "Deterring Complex Threats" Project
Funded By the U.S. Department Of Defense Minerva Institute

http://deterrence.ucsd.edu

Contents

INTRODUCTION 2
Panel 1: The Evolution and Future of Deterrence Theory 2
Panel 2: The Utility of Deterrence in Practice 5
Panel 3: Updates on Minerva Cross-Domain Deterrence Research 7
Panel 4: The Resurgence of Great Power Politics 8
Panel 5: The Impact of Cyberspace, Space, and Biological Technologies 9
Panel 6: Cross-Domain Deterrence and Nuclear Weapons 12
CONCLUSION 13

INTRODUCTION

In March/April 2010 the U.S. Department of Defense Office of the Undersecretary of Defense for Policy convened a 21st Century Cross Domain Deterrence Initiative (CDDI). The initiative brought together a group of prominent scholars and experts from outside government to assess how Cold War concepts of deterrence should be modified to address the contemporary threat environment. These discussions identified numerous challenges including how to issue credible threats given uncertainties about attribution and collateral damage, asymmetric situations in which the U.S. has more to lose than its adversaries, ambiguity about the laws of war regarding new modes of attack, and several other issues. The workshop at George Washington, six years later, was intended to reconvene the CDDI with several of the origins members and a number of new participants. This workshop was intended to invite participants to reflect on the relevance of the CDDI in light of the growth of cyber, space and biological capabilities and the emergence of Russia and China as key rivals and non-state groups as adversaries. It also was an opportunity to share recent research findings conducted by the "Deterring Complex Threats Project" led by Professors Erik Gartzke of U.C. San Diego, Jon Lindsay of the University of Toronto, and Michael Nacht of U.C. Berkeley.

The workshop was divided into six panels with a set of discussion questions to guide presentations. It was conducted under Chatham Rules with no attribution for particular remarks.

Below is a summary of the participants of each panel, the discussion questions, and a summary of the main points. A conclusion from the workshop is also provided.

Panel 1: The Evolution and Future of Deterrence Theory

Moderator: Michael Nacht
Participants: Richard Betts, Morton Halperin, Robert Jervis, and George Quester.

Questions
How has the complex 21st century security environment changed your thinking about the core elements of deterrence, if at all? Are the deterrence problems that appeared most challenging during the early Obama administration (i.e., the 2010 CDDI workshop) of greater or lesser importance today? Is "cross domain deterrence" a useful way to characterize 21st century deterrence? What is the most promising frontier for research on deterrence theory?

Summary of Discussion
Members of the first panel noted the limitations of applying the core elements of deterrence to the 21st century security environment, citing technological advancement in domains such as cyberspace; the advent of influential non-Western powers who perceive deterrence in a different manner; and the presence of adversaries with non-material prerogatives such as religion and martyrdom. In the globalized, complex 21st century security environment, panelists advocated the need for further discussion and research, especially with respect to cyberspace as part of a multi-domain strategy. Doing so would require building on historical precedent, and adapting

deterrence theory to account for cultural incongruences with allies and adversaries.

According to one panelist, the current generation of policymakers and scholars approach the contemporary security environment with greater creativity and open-mindedness than those in the Cold War era. This is a necessary evolution, as the core elements of deterrence formulated in the 20th century cannot adequately address the challenges faced in a post-Cold War world. On the one hand, there has been a globalization of security concerns. On the other, the complexity of recent technological developments--especially innovations in space and cyberspace--are difficult to grasp through a set of axioms devised in response to the danger of nuclear warfare.

Given the globalization of security concerns, one panelist suggested that it was important to have greater understanding of non-Western ways of approaching deterrence. Different cultures do not interpret deterrence in the same manner. Consequently, this could limit a policymaker's confidence in signaling as statecraft since beyond beyond the technical challenges; it is also likely that such efforts could be misread. Another panelist highlighted that while today's globalized security environment is more complex than the 20th century dominated by the US-Soviet rivalry, differing perspectives on matters of deterrence and manners in which states perceive conflicts existed during the Cold War as well. Recounting a meeting between American and Soviet policymakers at the end of the Cold War, the panelist said that in response to an American comment that at least Cold War conflicts did not go nuclear, their Soviet counterparts argued that all Cold War conflicts were in fact nuclear!

Such differences of perception continue to pervade the 21st century security environment. According to one panelist, today, cultural incongruence would be evident in any effort to address Chinese concerns. Unlike in the west, any crisis may be seen as a threat, but it is also viewed as an opportunity for the Chinese to assert themselves. Furthermore, non-material standards such as religion play a significant role in the calculations of many other adversaries in the complex 21st century security environment. As the panelist remarked, it is exceedingly challenging to deter an adversary who promotes martyrdom.

In this environment, one panelist suggested that "cross domain deterrence" becomes a useful way to characterize 21st century deterrence as it allows policymakers and scholars to see how the deterrence of an adversary could be more than a defensive strategy. The panelist cited current tensions with North Korea as an example, noting that the North Koreans use nuclear weapons as a shield. On multiple occasions in recent years, the North Korean defense establishment has executed high-risk moves without any significant retaliatory response from either the United States or South Korea. Approaching such challenges through the prism of cross domain deterrence facilitates the development of an effective response in the future, both short and long-term. Arguing that current theory has been unsatisfactory in explaining cyber threats and opportunities, one panelist suggested that cyberspace and cyber warfare in particular were promising frontiers for further research on deterrence theory.

Another panelist sought to provide some historical perspective in order to underscore the importance of the core elements of deterrence – especially with regard to nuclear weapons. The panelist noted that these core elements were developed by thinkers focused on the United States' relationship with the Soviet Union during the Cold War. They added that many of the challenges

of the mid-20th century continue to exist today. In particular, they noted the threats posed to the United States and its allies by an increasingly expansionist Russian state – strikingly similar to the threats thought to have been posed by the Soviets a few decades ago. As was the case with the Soviets during the Cold War, Russian-controlled nuclear weapons continue to deter the United States and its allies from making certain moves.

Moreover, the panelist suggested that any adaptation of deterrence theory to address current threats will need to continue to take into account how to avoid inadvertent nuclear war due to technological developments (including those in cyberspace) and subsequent military escalation "driving us there". Ultimately, adaptations to deterrence theory notwithstanding, the panelist argued that policies implemented to deter threats in the Cold War era – such as the ABM treaty – are just as important today, for anti-ballistic missiles are just as destabilizing as they were in the 20th century.

For another panelist, though technological advancement has increased the number of potential 'domains' of warfare, the concept of cross-domain deterrence itself was useful – and used – for deterrence in the 20th century as well. According to the panelist, American military advantages in both conventional and nuclear weapons allowed the United States to deter conventional attacks with nuclear weapons. The panelist suggested that any doctrine of "no first-use" was only put forth by the side with a distinct conventional advantage. Consequently, citing the importance many placed on maintaining a conventional advantage while technological advancement in cyberspace and other domains continued, the panelist stressed the utility of characterizing 21st century deterrence as "cross domain" deterrence.

The panelist suggested that cyberspace was but one aspect of a larger frontier for further research on deterrence theory. Invoking the historical example of discussions regarding the legitimacy of chemical warfare, the panelist argued that it is of utmost importance to ascertain how weapons in various domains interface with each other: how chemical weapons fit into a world with nuclear weapons, and the relationship between cyber and conventional weapons were two of the permutations the panelist cited. Another panelist argued that the absence of a declaratory policy with regard to the use of cyber weapons posed unique complications. According to this panelist, such complications were not present in the Cold War era due to the presence of declaratory policies for the use of nuclear weapons. In addition, the panelist noted that further research should not be restricted to understanding the interface of weapons systems, but also needed to take into account how to incorporate actions such as the imposition of economic sanctions.

One panelist stressed the need for policymakers and scholars to continually re-evaluate the same discussions that they have been having since the Cold War in the face of new threats. He added that a new challenge is the public's lack of familiarity with the status quo in new domains such as cyberspace, contrasting this with the greater public awareness of such security concerns in the nuclear domain during the Cold War. Another panelist suggested that in today's globalized security environment, such discussions should not be restricted to domestic views or bilateral concerns. Instead, future discussions will need to take into account the perspectives and potential cultural incongruences between the United States and other non-Western nuclear powers such as Russia, China, India and Pakistan – as well as adversaries such as North Korea.

Panel 2: The Utility of Deterrence in Practice

Moderator: Jon Lindsay
Participants: Francis Gavin, Charles Glaser, Avery Goldstein, and Barry Posen.

Questions
Is there a gap between deterrence theory and practice? If so, has theory missed important features of the policy process or threat landscape, or do policymakers not appreciate the nuances of theory? Have we learned the right lessons about how states used deterrence in the past, and what are the implications of these lessons for deterrence policy in the future? What are the boundaries or scope conditions for the use of deterrence to address the range of threats confronting policymakers today with the diversity of coercive instruments they have available?

Summary of Discussion
The discussion began with one panelist recognizing that deterrence itself cannot account for the actions and interests of the United States. He noted that US efforts go well beyond deterrence, and that deterring attacks on the homeland was never a serious concern. Instead, eight other motivations for American actions were cited:

1. Deterring attacks on US allies
2. Deterring certain allies from acquiring their own nuclear weapons
3. Deterring neutral states
4. Assuring allies they will not be abandoned
5. Assuring neutral states that the US is pursuing nuclear non-proliferation
6. Assuring adversaries that the US will restrain allies
7. Assuring both adversaries and neutral states that US capabilities are not oriented toward bolstering its first-strike capability
8. Defeating adversaries without war.

The panelist stressed that American possession and development of nuclear weapons was only partly aimed at strategic deterrence, concluding that this made the United States pursuit of nuclear weapons unique in the global landscape. According to the panelist, all other states acquired nuclear weapons primarily to protect the homeland and prevent invasion from adversaries.

With regard to the gap between deterrence theory and practice, one panelist claimed that there is a gap, and that this is ideal. They argued that the best theories rely on simplifications of the world. Another panelist agreed with this sentiment, and said that deterrence theory itself was not incomplete per se. However, challenges in the 21st century globalized security environment lent themselves to new applications of the concept of deterrence. In the current security landscape, one panelist noted that China was a particularly interesting case from the perspective of the United States. He suggested that China today was a more tempting target than the Soviet Union during the Cold War. This was particularly because the notion of damage limitation could now be considered – proliferation during the Cold War period was so great that damage limitation was essentially impossible. Consequently, the use of deterrence by nuclear-armed states in the past did not lead to any major implications of its relationship to damage limitation. The unexplored issue of damage limitation required more scholarly and governmental attention.

One panelist argued that China was an interesting case partly due to the state's proximity with the North Korean regime, and because a large conventional war was more of a possibility now than during the Cold War. The panelist remarked that a critical lesson from the Cold War era is that states do not necessarily pursue the defense strategy that theory suggests they should, noting that policymakers today may not necessarily appreciate the nuances of theory as well. The panelist said that this must be kept in mind as policymakers and scholars consider the boundaries and scope conditions for the use of deterrence to address threats with the increasingly larger range of available coercive instruments.

The panelist advocated for the institution of an effects-based doctrine. He added that more attention needs to be paid to the escalatory effects of attacks in emerging domains. The escalatory effects of attacks in cyberspace, for instance, remain uncertain whereas the effects of kinetic attacks are currently more predictable. Furthermore, the value of clarifying whether an actor did indeed originate a cyber-attack on an adversary remains unclear. This complicates efforts to determine the kind of retaliation such attacks in cyberspace necessitate, particularly with regard to prompt responses. The panelist suggested that an immediate retaliation may not always be the ideal course of action.

Moreover, the panelist argued that the complexity of retaliation – and thus, the application of deterrence – today is exemplified by the potential effects of imposing an economic attack through policy maneuvers. He said that an important area for further research would be determining how to differentiate among the effects of an economic attack, a cyber attack and a kinetic attack.

Another panelist suggested that the complications of devising an effective deterrence strategy in the current security landscape go beyond determining the differences between attacks in various domains. He argued that many theorists continue to recommend policies that not only fail to consider the complexities of the threat space and potential retaliation, but also do not take into account prerogatives in domestic politics – at home and for the adversary – as well as bureaucratic hurdles. As a result, the panelist suggested that even today, old patterns and misunderstandings continue to repeat themselves. As was the case with the Soviet Union, fundamental misunderstandings pervade the strategic calculations of both China and the United States: the US considered Chinese deployment of MIRVs to be an intentionally destabilizing act, while the Chinese only deployed MIRVs to counter a perceived threat from the US.

A further complication noted by a different panelist was that there is a lack of clarity in US policymaking circles on whether the US is trying to deter a particular actor. The panelist said that although it seems intuitive that policymakers should know when they are trying to change another party's actions or defend the status quo, it is not clear that this is always the case. Additionally, the panelist argued that analysts often incorrectly conflate deterrence and compellence. The panelist stated that the term "compellence" – demanding changes to the status quo -- is not used as much as deterrence, but is often a more accurate description of US policy.

Panel 3: Updates on Minerva Cross-Domain Deterrence Research

Moderator: Erin Fitzgerald
Participants: Erik Gartzke, Rex Douglass, Pat Schuster, and Eva Uribe.

Question
What are some findings from recent research in cross domain deterrence?

Summary of Discussion
One panelist began the discussion with a recount of the program's history. The Minerva Cross-Domain Deterrence Research Program is supported by the U.S. Department of Defense and was founded by then Secretary of Defense Robert Gates. He noted that the core intent of the program is to combine theory and practice to make deterrence more approachable for the community of interest and the general public. The research on deterrence should not be done in a vacuum and should be developed with frequent interactions with the community. The goal of the project is to focus on how different means for producing threats and actions have different effects on deterrence outcomes.

Another panelist said that deterrence as a definition is still unclear and bundles together a number of distinct objectives. It is most frequently used to indicate "something *against* the adversary". She noted that any conceptualization of deterrence contains a bias for the status quo, seeks to avoid conflict and intends to minimize costs. Emerging technologies have made some adversaries more capable. However globalization has increased mobility of populations and resulted in additional linkages that affect how nations determine their deterrence strategy. There is an ongoing debate about the domains of deterrence. The panelist argued that in the 21st century security environment, the interdependence of threat technology further complicates the conventional framework for deterrence. Instead of assuming a hypothesis, she said that it is important to collect data and provide evidence towards a new hypothesis.

According to one panelist, cross-domain deterrence theory is not new; however, it is increasingly applicable in the contemporary world. He noted that in the current security landscape, cross-domain deterrence now allows actors like China, Russian and Iran, and non-state actors to leverage emerging threat capabilities against their adversaries. Another panelist said that each nation varies in its comparative advantages in military strength. Societies that are bound together are more dependent on each other and give advantage to the party that is more willing to take greater risks. She added that their ability to deter an adversary will depend on individual events of conflict, understanding of trade-offs and bargaining power. The tools can be expensive, robust and specialized, or cost-effective, generalized and inefficient to counter new threats. She said that the question policymakers and theorists face is not what tool to pick, but how to determine which tool or strategy would be most effective.

One panelist said that policymakers in the U.S. seek to preserve national interests and minimize escalation by adversaries. They require a wide range of options with enough flexibility. The panelist suggested that it was important to consider the extent to which U.S. policymakers have thought about cross domain deterrence. The panelist himself held that cross-domain deterrence

has been a consistent feature of US defense policy. Comparing instances from the Cold War, the panelist said that when President Truman broke Stalin's blockade of Berlin in 1948, and President Kennedy sought to respond to the building of the Berlin Wall in 1961, a free Berlin was an important priority for the NATO alliance. He argued that cross-domain deterrence was essential in both cases: to assuage the concerns of allies in continental Europe, it was important to indicate that the US had the ability to act in the nuclear domain, and that the US was also ready to fight – and win – a conventional war. The panelist concluded by stating the necessity to further investigate the trade-offs between escalating versus stabilizing, and compare the effects of differing motivations such as religious or political goals.

Panel 4: The Resurgence of Great Power Politics

Moderator: Erik Gartzke
Participants: Eric Heginbotham, David Helvey, Olga Oliker, and Jason Reinhardt.

Questions
How do Russian and Chinese leaders think about deterrence in the 21st century? Is cross domain deterrence (by whatever name) relevant to their policy formulations and, if so, how? How do they use or seek to develop asymmetric means to counter the comparative advantages of the United States, and to what asymmetric means are they vulnerable? How should we expect them to manage tradeoffs and linkages across different means of influence and policy objectives in a crisis? What are the implications for U.S. deterrence policy?

Summary of Discussion
One panelist noted that the emergence of new technologies has allowed state actors like China, Iran and Russia and non-state actors to leverage their threat capabilities against the United States. He stressed the challenges posed by Chinese strategy. According to him, misdirection and ambiguity are key for Chinese adaptation of deterrence. They approach deterrence holistically – a combination of legal, psychological and media, commonly bundled as the 'three warfares'. The Chinese word for 'deterrence' also means compellence, better explained as coercion. He said that their emphasis on psychology, in particular the ability to confuse and confound their adversaries, is a growing challenge for U.S. policymakers and deterrence theorists.

According to one panelist, the Chinese government regards nuclear weapons as having limited utility. Any weapon that survives for a second strike has sufficient retaliatory capacity. The U.S. places significant emphasis on China's no-first-use policy and anti-access aerial denial (A2AD) policy. While they may not actively practice 'cross-domain deterrence', he said that their strategic alignment with lean nuclear warfare and increasing space interventions indicate their leverage across domains. He added that recent evidence suggests that China's focus is shifting toward building capabilities for high intensity defense, conflict with Taiwan with an underlying assumption of U.S. intervention, conflicts on their border with assumptions of international intervention and internal disruptions such as terrorism in Western China. It intends to avoid escalatory consequences and is improving early warning systems, indicating China's comprehensive integrated strategic deterrence policy. In light of a more capable force, the panelist suggested that it is possible the Chinese will revise the aforementioned policies and take a more offensive stance in the Asia Pacific.

Another panelist noted that on the contrary, Russia's doctrine emphasizes use of nuclear weapons for "escalating to de-escalate." Recounting the history of Russian defense policy following the collapse of the Soviet Union, he noted that in the 1990s, the Russians began to focus more on planning to use low-yield nuclear weapons for conventional war. However, nuclear weapons continued to act as the most effective deterrent for nuclear weapons. In early 2010, Russia was expected to raise its nuclear threshold and only use these weapons when faced with existential threats. Subsequently, however, the Russians revised their doctrine to introduce the concept of early use of nuclear weapons to deter NATO conventional responses, exemplifying their belief in the utility of cross-domain deterrence.

The panelist argued that it is evident Russia sees nuclear weapons as a political as well as a military tool. In the Russian language, 'deterrence' is defined as containment, much how the U.S. approaches it. It intends to "cause terror and fear". Citing Russian policy, another panelist said that are several asymmetries in deterrence across domains. He stressed that strategists should combine asymmetric threats in communication, credibility, capacity and calculations to develop an integrated and effective deterrence strategy. However, he noted that asymmetries are exploited in the face of hybrid warfare, and highlighted the importance of determining how an adversary can counter a deterrent threat using asymmetric means.

One panelist remarked that deterrence theory is often in conflict with operations. North Korea is unwilling to listen to China's concerns, while India regards China as an important adversary and is trying to push for parity. Russia continues to take nuclear weapons seriously, not only to deter its adversaries but also to retain its position as a superpower. By exploiting asymmetries across domains, he suggested that it might be feasible to deter adversaries without getting into a shooting war.

Panel 5: The Impact of Cyberspace, Space, and Biological Technologies

Moderator: Jon Lindsay
Participants: Benjamin Bahney, Daniel Gerstein, James Lewis, and Martin Libicki.

Questions
Do advances in information, space or bio technologies, including the military and commercial applications of those technologies, alter our conceptions of deterrence? If so, is the change due to new technologies that pose unprecedented problems or new concepts that may apply to familiar problems in unappreciated ways? How can the threats posed by these technologies be deterred? How can these technologies be used to deter threats? How does deterrence compare to defense, institutional coordination or some other strategy as a policy to mitigate these threats?

Summary of Discussion
Space
One panelist noted that space defense is expected to take a greater role in the 21st century, and the United States needs to pay close attention to how significant rivals such as China and Russia continue to develop their space forces and capabilities. The possibilities of smaller, more robust systems that are capable of surviving an attack offer a greater potential for defense in the space

domain. He suggested that this may create the potential for extending cross domain deterrence into the space domain in the future.

Another panelist said that the space domain is critical in overall US strategic policy and is inherently cross-disciplinary. He argued that this domain is vital to the proper operation of many different key US military systems, including nuclear command and control and conventional forces. Integration and cross-linking of these domains has enabled the United States to project power against adversaries and in regions identified as possessing strategic and national significance at any moment in time. He noted that this comes from the formidable capability of the US to conduct surveillance and reconnaissance missions with satellite and other means of space-based imagery intelligence (IMINT).

The panelist added that the constant streaming of intelligence from space-based intelligence provides a benefit to military forces whether deployed in conventionally large wartime operations or for smaller, more precise special-forces operations. This ability to gather and analyze real-time information also provides a first-strike advantage at the start of a conventional war. According to the panelist, China and Russia have recognized American space capability and have set their own goals for developing precision strike capabilities in space, making space a key part of their strategic focus. He also stressed the difficulty in defending orbital assets, and suggested that this was partly why the space domain remains offense-dominant.

A panelist argued that the space domain is potentially the least escalatory of all the domains discussed. He noted that strikes in the space domain have the least amount of or no causalities. Deaths, in particular civilian deaths, always register poorly in public opinion, thus making actions in the space domain potentially more advantageous given the low potential for civilian loss. Thus, he said that the use of military force in space could have a compellent effect on potential adversaries of the United States.

Cyberspace

According to one panelist, deterrence in cyberspace consists of four key elements:

1. The communication of a threshold to an adversary.
2. The adversary's assessment of the credibility of any threat of retaliation.
3. The possession of the means to deliver the communicated retaliation.
4. Accurate attribution for any cyber attack.

The panelist added that of these four elements, the US currently is most capable of delivering any communicated retaliation. He noted that after the public discovery of the Stuxnet worm against Iran, American threats in the cyber domain are taken seriously, and that the US has strong credibility. According to the panelist, the scale of damage caused should always be assessed in conjunction with who carried out the attack. He added that assessing the scope of a cyber-attack can assist the US in determining proportionality of the retaliatory response.

Another panelist suggested that the use of cyber attacks as one tenet of cross-domain deterrence is inherently destabilizing because both the domestic and international defense communities have yet to ascertain how to determine proportionality in cyberspace. The panelist suggested that the 2014 hacking of the Sony servers exemplified some of the attendant difficulties of conceptualizing proportionality and deterrence in the cyber domain. Following the hack, the US

needed to decide whether the intrusion of the servers of a private, multinational company with headquarters in Japan constituted an attack on critical American infrastructure. If the Sony servers were considered to be critical infrastructure, the panelist noted that it would be equally challenging to determine what kind of response such an attack warranted. In this regard, it was particularly important to consider American strategic priorities: the panelist questioned how retaliating against North Korea would influence North Korean aspirations to target South Korea in any domain.

The panelist also said that developments in the cyber domain posed a problem for relations with Russia and China. According to him, the Chinese and the Russians feel that the United States has developed a suite of weapons in cyberspace that can be deployed strategically without the US having to even consider the use of nuclear weapons. This has elicited Chinese and Russian suspicions, as both states believe that such technological developments belie an American attempt to undermine Chinese and Russian deterrent capabilities. The panelist noted that for the Russians in particular, such suspicions have been exacerbated by an absence of any meaningful cooperation or dialogue between the US and Russia on new developments in the cyber domain.

With regard to the efficacy of policies such as deterrence, defense and institutional coordination as means of mitigating threats in the cyber domain, one panelist argued that many such strategies could – and should – work in tandem in order to maintain a robust strategic position. The panelist said that developing a good cyber defense would dissuade adversaries from attempting attacks. As for deterring an attack itself, the panelist said that it was essential that the US build its capabilities to accurately attribute a cyber attack. He suggested that the US develop and subsequently present a credible ability to capture the tools used by any potential adversary and reveal them to the public. Such a revelation would force any adversary to undertake the costly process of developing new tools while simultaneously preventing the adversary from attacking different targets. The panelist concluded by offering a caveat: given that little that is known about cyber warfare, multiple and regular revisions would need to be made to any policy of deterrence as new capabilities are revealed--and created.

Biotechnology

One panelist said that there has been an unprecedented proliferation of biotechnology research and development over the last decade in both basic and applied sciences, ranging from the work of large biotechnology companies to people who conduct experiments out of their garage. He added that the resultant advances have driven significant change in technology and capability in this domain. This has led to the introduction of many dual-use technologies into the market. Consequently, he suggested that this increases the likelihood for non-state actors with an intent to harm the US because, with minimal training, a biological weapon could now be deployed in a relatively short period of time. This gives non-state actors capabilities akin to that of a state actor in this domain: the ability to create a biological weapon.

Another panelist highlighted the dangers this poses, as any deviant microbiologist could pose significant harm. He also suggested that deterrence, either within domain or cross-domain, is seemingly not possible against non-state actors since they operate outside the jurisdiction of treaties and laws of armed conflict.

In contrast, one panelist argued that biological weapons are strategic in a similar manner to that of nuclear weapons, and that a cross-domain deterrence framework can be applied. However, a different panelist stressed that the US is not well suited for deterrence in the domain of biotechnology. This panelist supported his claim by commenting on recent outbreaks of diseases like Ebola and H1N1. He said that the lack of preparation and slow response to deal with these outbreaks clearly demonstrate the US is not capable of dealing with an advanced or sufficiently esoteric outbreak, let alone a biological weapon attack. Commenting on this slow response, he added that if the US were not better prepared to address a biological weapons threat, efforts by the US to deter adversaries in this domain would not be effective.

Panel 6: Cross-Domain Deterrence and Nuclear Weapons

Moderator: Paul Nielan
Participants: Joseph Pilat, Robert Vince, James Walsh, and Nick Wright.

Questions
Is the proliferation of multiple threat technologies to regional actors changing traditional deterrence considerations? How might regional actors use cross domain deterrence either in lieu or in combination with nuclear threats? What is the strategic role of latency in cross domain deterrence? How should U.S. deterrence policy adapt to deal with the stability-instability paradox that appears to be operating in many regions?

Summary of Discussion
According to one panelist, the doctrine of nuclear deterrence that persisted during the Cold War cannot continue in its same form into the 21st century. The world simply has more players involved than the two ideological blocs of the USSR and the US. Countries like South Korea and Japan, which have relied on reassurance from the US in the past, are now taking a more active role in their own defense against neighboring, adversarial nuclear weapon states, especially North Korea and China. This brings into play complex and often disparate motivations including culture, religion, and ideology, all influencing their decision-makers' political decisions and their determination of cost in a given situation. The panelist said that this necessitates an open dialogue and transparency between the US and the state in question, be they ally or adversary, adding that this may not always be feasible.

One panelist was doubtful that a new age of proliferation of nuclear weapons was imminent. He noted that the number of states considering nuclear weapons programs has shrunk in recent years. He also stated that the type of state pursuing nuclear weapons has changed in the 21st century from the Cold War Era. During the Cold War, states that sought nuclear weapons were well-developed and technologically sophisticated. In recent years, the states seeking nuclear weapons are far less developed and technologically advanced. The panelist argued that modern proliferators seek weapons as a means of stabilizing their governing regime and, in some cases, deterring U.S. conventional intervention.

Another panelist suggested that strategic latency must not be overlooked. Strategic latency seeks to identify which technologies, if developed and deployed by an adversary, could cause significant threats to the national security of the US. He said technologies coming through the

research and development pipeline as well as technologies already deployed in the private sector that could be repurposed for an adversarial nation's needs both pose emerging threats. He noted that this problem is further compounded by the proliferation of dual-use technology. A relevant deterrence framework will require more evidence to prove that an adversary purchasing dual-use technology has malicious intent against the US.

In order to anticipate an adversary's moves to deter it in either intra- or cross-domain circumstances, one panelist contended that understanding human psychology is critical. Prediction error, or the psychological impact of surprise, was highlighted by responses to the London Blitz during World War II. During the interwar period, strategic bombing of cities was predicted to have a significant psychological impact on citizens that would drastically reduce the morale of the citizenry, resulting in faster capitulation of the state. This, however, was not the case during the London Blitz, as Londoners and the rest of Britain rallied with new vigor to resist Germany. The panelist argued that this was partially attributable to underestimating and misinterpreting the psychological impact on the populace. Due to this fact, another panelist suggested that cross-domain deterrence could be very effective at controlling the level of an adversary's surprise by engaging them in different domains. This could create a strategic advantage, giving the US the ability to escalate and de-escalate a situation depending on the need.

CONCLUSION

The panel discussions pointed to a number of key areas for further research. They included:

1. In depth understanding of the elements of cyber deterrence with limited attribution capabilities.
2. How cyber deterrence calculations might be altered if attribution capabilities improve markedly.
3. Conditions under which cyber attack would warrant cross-domain responses.
4. The role of damage limiting technologies in cyber and space.
5. Renewed efforts to defend against and deter major biological attacks.
6. Greater understanding of the meaning of proportional responses in a complex security environment with weapons capable of use in multiple domains.
7. Greater understanding of means of escalation and escalation control in a cross-domain environment.
8. Improved understanding of deterrence calculations by adversaries and potential adversaries.
9. Greater focus on the psychological effects of potential attacks in different domains in a variety of cultures using red teaming and other simulation techniques.