Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain

Maj Gen Susan J. Helms, USAF
Director of Plans and Policy
US Strategic Command
Offutt AFB, Nebraska

In May, a large team from US Strategic Command (USSTRATCOM) participated in Schriever Wargame 2010 (SW 10), hosted by Air Force Space Command (AFSPC) at Nellis AFB, Nevada.

The Schriever Wargame series is the AFSPC commander's game, designed to examine space and cyberspace operations in depth. The wargame allows participants to consider the diplomatic, economic, informational, and military influences that will shape deterrent strategy and defensive operations for space and cyberspace. It provides information for future requirements, examines organization constructs, and provides a venue for advancement of space and cyberspace policy and rules of engagement. Although SW 10 was a service wargame, USSTRATCOM has been a key mission partner of the series since its inception 10 years ago.

An important conclusion we have drawn through the experience of the Schriever series is that some lessons about deterrence from the Cold War era do not necessarily translate to the space and cyber realm.

A critical objective of SW 10 was to examine how to wage deterrence in space and cyberspace, and to explore integrated planning processes that employ a comprehensive, "whole of nations" approach to execute operations across multiple domains. Other objectives of the wargame were to demonstrate strategic posture and resolve, and to effectively conduct strong coalition operations to, if necessary, recapture the initiative in space and cyberspace.

Building upon previous wargames of the Schriever series, this year's wargame provided the opportunity to expand on previous lessons, test new concepts, and importantly, to incorporate new elements of integration across space and cyber, functional and geographic combatant commands, government and industry, Department of Defense and interagency, and the US and her allies and partners.

From the very first move of the wargame, the entire scenario served to remind us all how difficult it can be to think through and implement an effective deterrence strategy to forestall a crisis.

The year was 2022 and, in response to a perceived provocation, a regional adversary disabled the cyber and space assets of a key US ally. Over the course of the next four days of the wargame, the crisis escalated to the senior executive level, and soon encompassed us all, including partners beyond our own government and nation. Interagency leadership gathered to weigh in on how to counter and deter future conflict—and how to coordinate actions among multiple nations to achieve the best effect.

Throughout the process, as we and our allies debated about what to do to deter the adversary from threatening our space and cyberspace capabilities, it became clear that the enemy was not deterred from further escalation. As we came to learn, the leaders of this provocative regional state had defined their objectives (although those objectives were not obvious to us) and had already thought through the overall costs and benefits of their plan. In other words, they had assessed our likely behavior in the context of the scenario at hand, determined that, for them, the benefits of action outweighed the risks and they made their decision to "move out." At that point, options for deterrence by the US and her allies were "late to need."

As a coalition, what *were* the options?

Could we take some actions that would de-escalate the conflict and return to status quo? Was there a way to encourage restraint, such that the flashpoint scenario that began the wargame could dissipate? What did the adversary actually want, and what were they willing to incur as a cost to get it? Had they analyzed in advance the most likely responses of the coalition once they "kicked over the anthill"—and did we behave just as they had assessed we would? If so, then we were unwittingly and obediently following a script that the adversary had already written for the campaign, and our military actions to deter would have no effect on their decision calculus. The predictability of our response—and their accounting for it—was a part of their cost/benefit trade space well before they made their first move.

Principles of Deterrence

Effective deterrence is extremely difficult to plan for and execute after hostilities appear imminent. An effective deterrence strategy is not one that is defined by actions within one domain, or one area of responsibility, or one nation. Deterrence cannot be an invisible strategy, for a core premise is that an enemy is influenced by actions and messages that can be perceived—and

Over the course of the next four days of the wargame, the crisis escalated to the senior executive level, and soon encompassed us all, including partners beyond our own government and nation.

conveyed in advance.

To be effective at the strategic level, deterrence must be viewed through the lens of how your adversary views the geopolitical world, and that can be a very complex thing to comprehend. Deterrence is not static; effective deterrence strategies will morph under conditions of crisis, and the level of uncertainty about your adversary's decision process must be actively tracked and accounted for, or else you risk serious miscalculation and unexpected deterrence failure.

The Challenge of Space and Cyber Deterrence Objectives

In the decades-old nuclear framework, deterrence objectives are geared toward influencing the political perceptions and military choices of your adversary. The objective of *nuclear* deterrence is to deter an adversary from using nuclear weapons. Having a confident comprehension about the beliefs, goals, values, politics, and motivations—on both sides—is a daunting challenge, yet highly important to develop an effective deterrence strategy. It is also a high stakes endeavor, due to the risks of miscalculation.

However, in spite of all of the complexities that make up the equation of a national leadership's decision calculus, there is one simple point of clarity about nuclear deterrence that transcends all of the variables: your deterrence objective is to convince your adversary that his least bad option is to exercise restraint.

In other words, in the nuclear framework, the complicated questions are not about *what* to deter, but *how* to deter. The strategy to deter a decision to cross the nuclear threshold will be scenario-specific and highly complex, especially in crisis, but there is really no ambiguity surrounding the goal of your deterrence objective.

An additional simplicity is that the nuclear threshold serves as a universal "pass/fail standard" for deterrence that any political leader can understand. Given the scale and scope of the consequence, it would not be difficult to recognize that your adversary has made his decision.

Beyond the relatively obvious kinetic thresholds, the discussions to date on space and cyber deterrence objectives do not have similar clarity. What exactly are the deterrence objectives on a non-kinetic battleground? Is the objective to deter "use" of space and cyber "weapons," to deter "attacks" in the space and cyber domains, or to deter notable disruptions of our space and cyber networks? Or is it really all about deterring any type of attack, kinetic and non-kinetic, on the US and her allies?

In essence, a deterrence strategy has to be built on a common understanding of what decision you are explicitly attempting to influence. Until you can put clarity on *what* to deter, there will be no clear or effective strategy on *how* to do it.

Let's say that our objective is to deter use of a kinetic antisatellite weapon against space-based platforms: that objective is generally easy to measure for success or failure, as the debris cloud that would ensue will catch everyone's attention and serve as a focal point of righteous global outrage. However, what if the satellite just quits working? The effect is the same, in that you cannot use the satellite for its intended purpose, but the means by which the satellite is no longer available changes the entire context of your deterrence objective.

In fact, your objective is really to deter *any* attack on a US satellite, kinetic or non-kinetic. Assuming you can prove to yourself that an adversary actually has a hand in this issue, then you need to broaden the scope of your deterrence strategy. That is, rather than defining the deterrence context to a narrow dimension—kinetic antisatellite threats and the associated costs to an adversary of space debris—your deterrence strategy should include other significant influencing factors in order to deter a potential adversary effectively.

Attribution and Other Factors

The challenge of attribution faced by the cyber forces in SW 10 was indicative of the significant "grey areas" involved with deterrence objectives in the non-kinetic domain. The deterrence objective was to generally deter "disruption of the network," but "disruption" is not a "binary" situation in the space and cyber realms.

Figure 1. Schriever Wargame 2010: Senior Leadership Seminar involving military, civil, and industry leaders.

Given the spectrum of effects achievable by non-kinetic means—from massive disruption to unnoticeable—the attribution and assessment challenge varies from trivial to likely impossible. Having the situational awareness to fully characterize disruption is not a certainty, depending on both the disruption effects and the means to monitor the situation. And if the effects were fully intentional, then who was behind it?

We are all aware of the challenges of attribution, and yet the measure of your deterrence campaign's success or failure depends on it. Without confidence of attribution, how do you credibly assure an adversary in a pre-crisis environment that you intend to respond? How do you mitigate the risk of a third party exploiting the ambiguity to create or escalate the crisis? How can you assess the success of meeting your deterrence objectives and adjust your adversary-focused campaign accordingly, if you are not confident about attribution?

To further complicate the situation, our tolerance for disruption will adjust depending on both the crisis environment and the scope and duration of the outages, which could undermine the credibility of the resolve we intend to communicate well ahead of the crisis. There are an infinite number of scenarios that are neither indicative of a minor harassing incident of jamming nor strategic attack. For non-kinetic activity, we have yet to articulate a well understood threshold for a space and cyber deterrence objective set.

Unfortunately, we are not helped by a culture that passively accepts occasional disruption of our networks as a way of life. However, the incredible complexity of the operating environment does not alleviate the imperative to think through clear geopolitical deterrence objectives and effective strategies to implement them.

The Challenge of Space and Cyber Deterrence Strategies

There is a pervasive assumption that the strategy lessons learned from nuclear deterrence in the Cold War can be directly imported to space and cyber mission areas for implementation. The relative simplicity of the Cold War, with its glacial standoff between just two primary actors, enjoyed the advantage of a shared understanding about mutual cost imposition, and a nuclear force structure that was designed to ensure stability in the balance of power.

The Nuclear Scenario

Consider the premise of the nuclear cost/benefit trade space. Nuclear weapons have prompt, massive destruction effects, and the general point of using them first is as a last resort weapon to achieve strategic political objectives, most notably in situations of an existential threat.

However, using nuclear weapons comes with an incredibly high bar for "benefits of action," generally because the costs of your decision will likely provoke nuclear retaliation by your enemy or their allies. In a conflict that has not escalated to the nuclear threshold, a nation would be strongly motivated to exercise self-restraint, thereby preserving nuclear deterrence.

Even in this relatively simple deterrence strategy example of "costs of using nuclear weapons outweigh the benefits of using nuclear weapons," the strategy analysis required to avoid miscalculation in both the Soviet times and in today's geopolitical environment is immensely complex and has always required a deep intellectual investment.

The Cyber and Space Scenario

In developing strategies for space and cyber deterrence, the entire context in these domains is different from the nuclear balance equation. Space and cyber capabilities are generally new means of technology to perform the age old function of command and control and situational awareness, not to create prompt destruction and horrific effects. This warrants a thorough, deliberate, nationally important discussion, for there are many strategy lessons that will not necessarily translate to space and cyber applications without careful consideration and adjustment.

As was mentioned often during the wargame, the space and cyber attacks and the motivations behind them were more about disruption than mass destruction. As such, they could easily be perceived as attempts to create an environment of disruption for information flow and imposing the "fog of war" in an asymmetric manner. Confusing your adversary, if you have the means, is not only a highly intuitive benefit, but also a sound element of traditional military strategy to achieve strategic objectives. Because of the lack of precedence and the wide variance amongst nations on space and cyber dependence, the costs you could possibly incur along with the supposed benefits of disruption are not nearly as intuitive as they are with nuclear weaponry.

It is a calculation that depends on a complex web of scenario-specific factors: the resilience of operations to a non-kinetic attack, the scale of the effects created, the state of declaratory policy, the credibility of a threat of escalation, and so on. It is both more complex and more uncertain due to a lack of precedents, compounded by issues such as attribution.

Ambiguity can have a role in the achievement of our deterrence objectives, but the strategy must be maturely formed, effectively influential in reference to your opponent's perceptions, and implemented well ahead of the adversary's decision cycle.

Implementing a deterrence strategy after the fight has already begun is utterly "late to need." To be effective, a deterrence strategy for the space and cyber domains must somehow relate to enduring standards that are understood by all sides before crisis.

Space and cyber capabilities are generally new means of technology to perform the age old function of command and control and situational awareness, not to create prompt destruction and horrific effects.

Depending on the adversary, the deterrence strategy may or **may not** include cost imposition options that are delivered by space and cyber forces. It will depend on whether those options have any deterrent value in the mind of your adversary—and whether he believes you would actually use them in the scenarios that he has laid out in his campaign. It is a critically important point: unlike the mature strategies developed over the years in the nuclear paradigm, the threat of sophisticated space and cyber options does not necessarily deter your adversary from using the same type of military capabilities.

Creating disruptive effects by leveraging space and cyber capabilities will certainly have military value, but whether it forms the basis of a viable deterrence strategy is an entirely separate question. The most effective strategy to deter crippling non-kinetic effects may not be to deter the use of space and cyber capabilities, but to deter the entire conflict before it begins, because the benefits of utilizing such capabilities in conflict may not be counterbalanced with costs meaningful to the adversary.

Conclusion

Thanks to our long history of deterrence thought and our national energy to make the necessary cultural adjustments, space and cyber deterrence concepts are clearly evolving in positive ways. However, nuclear deterrence concepts that worked very well during the Cold War and still work extremely well today do not always translate in practice to the space and cyber domains.

At the same time, the fundamental behavioral principles on which classical deterrence theory is based are still valid when applied to the nuclear as well as cyber and space domains:

- The need to know and inform in advance;
- Motivation of an adversary—what the adversary values, and what would be unacceptable costs;
- The importance of making deterrence effective with other means, such as strategic communication, to communicate a clear message of intentions and limits. Strategic communication can play a reinforcing role in communicating our intentions to the adversary as well as broader publics. In the information age, enlisting broader popular support may play as great a role in affecting an adversary's behavior as flexing military muscle.

Finally, areas of increased complexity in the space and cyber domains—attribution is the most salient example—are becoming potentially more complex than in the nuclear age, where we had grown accustomed to a single clearly defined adversary and threat. The challenge of asymmetric threats posed by rogue groups and non-state actors that may acquire weapons of mass destruction is a sobering adjustment to classical deterrence study.

Based on observations during the SW 10, this article has attempted to highlight some initial thoughts on where the differences lie. The discussion here has noted where it might be necessary to make some modifications in our approach to objectives and the strategies to implement them, while posing additional questions that will be fertile ground for future wargames.

The Schriever Wargames provide an opportunity for space and cyber professionals to experiment with "lessons observed" from previous games and real world scenarios in a penalty-free environment where "out of the box" problem-solving methods can be used. Many of these methods, if successful, can translate directly into real world policies and practices as "lessons implemented."

And that is the ultimate objective of conducting these wargames—to prepare our leadership and our warfighters for the day when the game may no longer be just a game. The invaluable opportunity of SW 10 enables us all to become a more agile, adaptable, and effective force in today's high technology global environment.

Maj Gen Susan J. Helms (BS, Aeronautical Engineering, US Air Force Academy; MS, Aeronautics/Astronautics, Stanford University, California) is director of plans and policy, US Strategic Command (USSTRATCOM), Offutt AFB, Nebraska. She is directly responsible to the USSTRATCOM commander for the development and implementation of national security policy and guidance; military strategy and guidance; space and weapons employment concepts and policy; and joint doctrine as they apply to the command and the execution of its missions. She is also responsible for the development of the nation's strategic war plan, strategic support plans for theater combatant commanders, and contingency planning for the global strike mission.

General Helms was commissioned from the US Air Force Academy in 1980. She has served as an F-15 and F-16 weapons separation engineer and a flight test engineer. As a flight test engineer, General Helms has flown in 30 types of US and Canadian military aircraft. She has also served as project officer on the CF-18 aircraft as a US Air Force exchange officer to the Canadian Aerospace Engineering Test Establishment.

Selected by NASA in January 1990, General Helms became an astronaut in July 1991. On 13 January 1993, then an Air Force major and a member of the space shuttle Endeavour crew, she became the first US military woman in space. She flew on STS-54 (1993), STS-64 (1994), STS-78 (1996), and STS-101 (2000), and served aboard the International Space Station as a member of the Expedition-2 crew (2001). A veteran of five space flights, General Helms has logged 211 days in space, including a spacewalk of eight hours and 56 minutes, a world record.

General Helms commanded the 45th Space Wing at Patrick AFB, Florida. Her staff assignments include tours at Headquarters Air Force Space Command and Air Education and Training Command.

The conclusions and opinions expressed in this document are those of the author cultivated in the freedom of expression, academic environment of Air University. They do not reflect the official position of the U.S. Government, Department of Defense, the United States Air Force or the Air University.