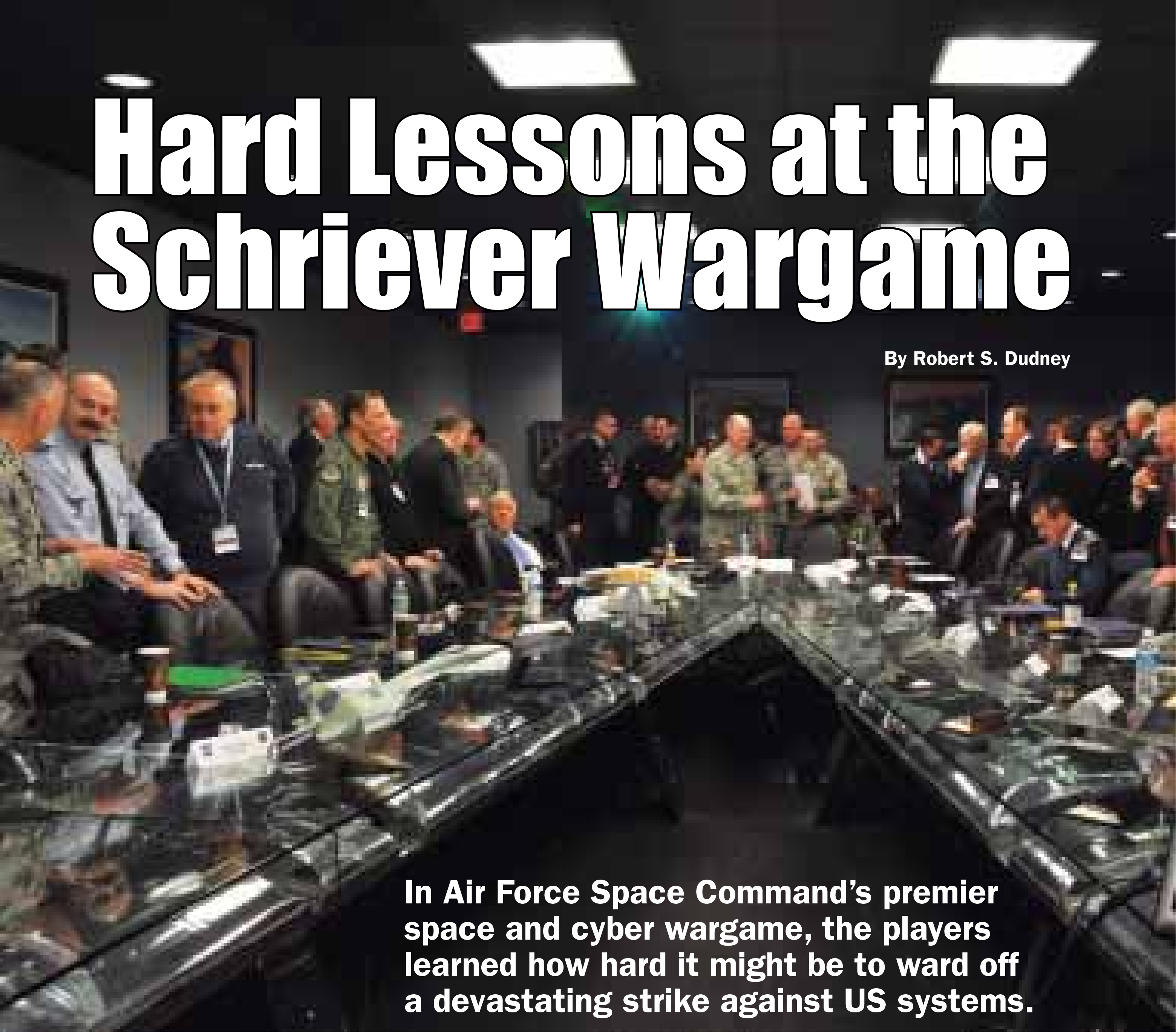
Hard Lessons at the Schriever Wargame

By Robert S. Dudney



In Air Force Space Command's premier space and cyber wargame, the players learned how hard it might be to ward off a devastating strike against US systems.

The global space and cyber war of 2022 started out small, in a corner of the Pacific. One of America's allies in the region engaged in some sort of local action. A US "peer" adversary—and China would certainly seem to fit the description—viewed that action as a severe provocation.

The peer responded violently. It swiftly knocked out the US ally's cyber and space systems, crippling it. Tensions escalated, and the next move was Washington's.

So began Schriever 2010, the latest edition of Air Force Space Command's premier wargame. The scenario did not include specific nations. However, US military personnel simulated what they thought could happen in the space and cyber realms a decade hence. The objective: Learn how to deter war in those domains.

The classified game featured some 600 military, civilian, and allied players. It unfolded over four days last May at Nellis AFB, Nev. Recent briefings, interviews, and articles have begun to lift the veil on some key conclusions.

Among them: Combat in space or cyberspace can instantly go global. Conflict in those domains cannot be isolated from other domains. Cold War-era deterrence theories are ill-suited for the space and cyberspace worlds of the near future. "From the very first move of the wargame," said Maj. Gen. Susan J. Helms, a player, "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."

According to participants, the game's world of 2022 will be extraordinarily complex. It would be inhabited by peer space and cyberspace competitors, as well as rogues. Civilian and commercial interests will be engaged. Vital assets could be hit with all types of weapons, kinetic and nonkinetic.

Following the game's opening gambits, things moved fast. The US ally invoked mutual defense agreements, and Washington responded positively to its entreaties.

The US response started a new dynamic. As some of the briefings show, the China-like "adversary" then took

SIDC Visualization Lab photo by Dan Santistevan

Senior military and civilian officials discuss the Schriever wargame during a break at a planning meeting in Washington, D.C.

pre-emptive action, focusing on denying US and allied access to space and cyberspace enablers, vital to any successful US military action such as air or naval operations in the Western Pacific.

This was described in one Air Force Space Command briefing as "Red Blockades Blue." The next move was "Blue Responds." In the next phase, the two sides engage in what was described as a "Major Attack."

Lt. Gen. Larry D. James, then commander of 14th Air Force and its Joint Space Operations Center at Vandenberg AFB, Calif., was a key participant. In a recent issue of *High Frontier,* the journal of Air Force Space Command, the general outlined some of the problems the US faced.

One was the fiercely assertive behavior of Red, the "peer" nation's leadership. "The adversary attacked aggressively, deliberately, and decisively on a variety of vectors to deny US and coalition forces access to space capabilities," James wrote.

In addition, James said, adversary forces had "a significant offensive advantage against US space capabilities" in the game. They executed "counterspace operations" at the time and place of their choosing, with little warning, he said. US decision-making and responses, in contrast, lagged badly.

This was more or less baked into the scenario, according to Col. Roger M. Vincent, commander of USAF's Space Innovation and Development Center at Schriever AFB, Colo.

"We had a much smaller group making decisions for the Red," said Vincent. "They clearly had in their minds certain trip points, what they were going to do. We portrayed Blue more like the decision apparatus of the United States."

In Washington, it seems clear, many more players were involved, and thus decision-making took longer.

Worse, said James, the US and coalition forces had only a limited ability to reconstitute those space forces that had been targeted. In fact, he noted, Blue "suffered from significantly degraded

Illustration by Erik Simonsen

A ground-based laser "blinds" an intel satellite in orbit in this artist's conception. One question asked at the game was what constituted a "red line" in space.

SIDC Visualization Lab photo by Dan Santistevan

Retired USAF Gen. Lance Lord, a former head of Space Command (l), and Gen. Robert Kehler talk over the wargame at the planning meeting. Kehler led AFSPC at the time, but has since been confirmed to head US Strategic Command. The exercise taught participants that the US should not try to go it alone in space.

space capabilities during the conflict and well into the post-conflict period." Helms, who at the time of the wargame was the director of plans and policy at US Strategic Command and who has since been confirmed to be the new commander of 14th Air Force, noted the swift escalation of the conflict. Over four days, "the crisis escalated to the senior executive level, and soon encompassed us all, including partners beyond our own government and nation," she said.

US interagency leadership, Helms continued, "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." However, "the enemy was not deterred from further escalation," Helms wrote in an article in *High Frontier.* Red simply continued to attack time after time.

"The leaders of this provocative regional state had defined their objectives ... and had already thought through the overall costs and benefits of their plan," said Helms. "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.' "

In one postgame assessment, several USAF officers from Pacific Air Forces offered a bleak view of US command and control in the game. "As the adversary challenged our access to space and cyber critical enablers," they wrote, "it was difficult for military leadership and the National Security Council to appreciate and predict the full impact of those actions."

They added, "At one point, ... it became clear that we had better intelligence and understanding of the state of Red's C2 than we had of our own systems."

Evidently, the attacker's specific objective was never totally clear. As Helms noted, it appeared to the Blue side that "the space and cyber attacks and the motivations behind them were more about disruption than mass destruction."

Disruptions to Deterrence Efforts

One could easily perceive them as "attempts to create an environment of disruption for information flow" and to generate a thick "fog of war" to weaken US capabilities, she said.

Without doubt, space and cyberspace assets give US forces critical capability to see, communicate, navigate, and operate in superior ways. Current and future adversaries recognize this and will almost certainly seek to deny those capabilities in time of conflict, said Air Force space officials.

"If you are a logical adversary, you say, 'Well, if I want to slow that juggernaut down, it probably is to my advantage to reach out and touch those information things that we are using to great advantage,'" said Kurt Nelson, a contractor supporting the Schriever wargame. "You could logically expect, in a crisis of the future, for someone to be dithering with your information systems."

In a recent study, RAND Corp. space analyst Forrest E. Morgan said a combination of factors "suggests that first-strike stability in space is eroding." Morgan added, "With a growing number of states acquiring the ability to degrade or destroy US space capabilities, the probability that space systems will come under attack in a future crisis or conflict is ever increasing."

This could happen in ways both standard and exotic, if the actions analyzed in Schriever 2010 are any guide.

A science and technology cell led by Werner J. A. Dahm, then chief scientist of the Air Force, considered various small, micro, and nano satellites.

Dahm reports that he emphasized the adversary's possible use of "grappler" satellites. Such satellites attach themselves to a target spacecraft, changing its momentum and center of mass, inducing drift and tumble while robbing the satellite of ability to control and orient its motion. Dahm said the game analyzed small satellites "designed to provide an on-demand kinetic kill capability" and "microwave-based directed energy capabilities to degrade or destroy the target satellite."

The challenge of coming up with effective policies and strategies to deter attacks or limit their effectiveness was only too apparent in the wargame.

The first problem was the congested nature of the space and cyberspace realms. With so many players—nations, companies, criminals, military units, hackers—on the scene, it was hard to know who was doing what to whom and why.

"We found that it is difficult to conduct attribution for actions in space," James noted at a recent US Strategic Command conference, where he discussed aspects of the wargame.

"Certainly, if there's an ASAT launch or something like that, generally we can see that and know what's going on, but if there are on-orbit objects that perhaps have been there for months or years, we ... can't necessarily know what their function is. How to attribute an action, based on what that object does? It can be very difficult."

Space Command currently tracks more than 20,000 objects and performs conjunction analysis on more than 1,000 satellites each day. Even more difficult is knowing the intent of a spacecraft's operator.

Equally disruptive to deterrent efforts in the game was a lack of clearly demarcated "no-go" zones or trip wires which the enemy knew he had to honor and avoid.

"What are the red lines in space?" James asked rhetorically. "How does an adversary understand what our red lines are as we operate in the space domain? Is jamming a satellite a red line? Is destroying a satellite a red line? There was a lot of debate at Schriever about that."

As several space officials tell it, the adversary seems to have frequently misunderstood Blue signals about what was or was not off-limits.

Beyond the problems of attribution and red lines, the matter of proper response and escalation came up time and again.

"We saw that what is a regional conflict when you start conducting operations in space ... can rapidly become more than a regional conflict" if you start "removing capabilities in space," said James. "How do you contain something to a region when space assets are global in nature and strategic in nature?"

Vincent, whose office was responsible for setting up and running the game, put it a different way.

"With some of our strategic nuclear systems, we've told the world, 'You touch those, we are going to respond accordingly,'" he noted, adding that with nuclear weapons, there is a clear threat of retaliation. "Cyber is a domain where we have to figure out what that means. It might be we can't [respond fully], because the cyber domain is ... so global. Once you hit the [global information grid], you're everywhere."

The prospect of collateral damage within the web of space and cyber systems was of concern to former Rep. Tom Davis, a Virginia Republican, who played the part of the President in Schriever 2010.

"Choosing to initiate an attack, cyber or otherwise, would disrupt this web with inevitable—and potentially significant—adverse effects to both aggressor and victim," said Davis. "Increasingly, a no-holds-barred approach is simply not an option."

Indeed, said Nelson, the lesson is obvious: The space-cyberspace theater is global, and can't be limited. "Whereas, in air, land, and sea, I can confine my fight to a theater, to a geographic area, and there are natural firebreaks there, in space and cyberspace there are no natural firebreaks," he warned. "This underlies our current rules of engagement. We've realized that I can start a fire here, and pretty soon it's everywhere."

Officials who took part in Schriever 2010 believe it yielded important conclusions about how to build deterrence in space.

One big lesson, said officials, is that the US military should not try to go it alone. A comprehensive system pulling in many different contributors from around the world adds depth and strength to the nation's space and cyber infrastructure.

Maj. David Manhire, SIDC's deputy director, pointed to the existence of five major groups in the wargame: the US military (combatant commands, Pentagon officials, the services); the commercial space and cyber industries; allies (Britain, Canada, and Australia); other US agencies (Departments of State, Homeland Security, and others); and the US Intelligence Community.

Of these five elements, Manhire noted, four fall outside of US military control, making wide cooperation essential. The idea is, should the US lose some of its capability, it would be able to fall back on others.

Consequences, Reactions

Joseph D. Rouge, then director of the National Security Space Office, told the STRATCOM audience that the US should become "selectively interdependent" with commercial and foreign operations. In that way, any attacker would have to ponder the fallout from unwanted collateral damage.

"When an attack on one is an attack on all, it becomes much more difficult to take on one of the partners, without taking on all," said Rouge. "I think that is a very key part."

For these reasons, many are pressing to develop a "space order of battle" that includes both commercial and foreign space systems. Even more important: further development of a so-called Combined Space Operations Center, or "CSpOC," to direct space and cyber moves in a war. In the wargame, foreign and commercial space officials joined in CSpOC deliberations, generating what James called "one of the clear successes" of the exercise.

The game also highlighted the need for much greater space situational awareness, officials said. Davis put the matter as bluntly as any: The Commander in Chief "likely will not initially know who is initiating the assault. … What would global reaction be to retaliation if the identity of the aggressor was in doubt? It is safe to say it would be unpredictable, at best."

James noted many events, even natural ones such as solar maximum events, can cause disruption. "Unless you have some sort of sensor that tells you this was indeed caused by solar activity, how do you know that that action wasn't taken by an adversary with something that you couldn't see?"

The upshot: If the US can positively "finger" an attacker, then it can credibly threaten retaliation. If the threat of retaliation is credible, deterrence might hold. As many officials see it, the game also demonstrated the need for much stronger and detailed declaratory policies about space and cyber issues.

Vincent said the game participants "had quite a few conversations" about establishing red lines, trip wires, and "keep-out" zones, as a way of warning an adversary away from tampering with the Blue team's "crown jewels" in space and cyberspace. "If you don't articulate those red lines to the adversary, they will never know when they get close," said Vincent. "If they don't know when they're close, how can they be deterred?"

Rouge called for a major effort to "develop and enhance norms of behavior in space." With that, he said, must come plans for rewarding space operators who follow these rules and dealing with malefactors. "One thing we learned at Schriever," said Rouge, "was that we can't afford to do it ad hoc." Planning for retaliation in space or cyberspace "requires something like a DEFCON system" that has applied in the strategic nuclear world. Rouge said there should be "an automatic response" laid out in the wake of any decision to escalate.

"We need to give rules of engagement to our field commanders," said Rouge. "What can they do? What can't they do? The enemy needs to understand that they're going to get a consequence, that they're going to see a reaction."

Space officials are quick to note that the situation is neither desperate nor beyond repair. They emphasize the wargame postulated threats which might be a decade or more in the future.

According to Nelson, it is not accurate to say "this has become an Achilles' heel, and a single swing from a single sword" is going to take down the US military space setup.

However, "if we continue along the trends that we see, we may find ourselves in the near future arriving at a place where we do indeed have this Achilles' heel," Nelson said. ■

Robert S. Dudney is a former editor in chief of Air Force *Magazine (2002-2010). His most recent piece was "The Lavelle Syndrome" in the September 2010 issue.*