AIR FORCE SPACE COMMAND

Volume 7, Number 1

HIGH FRONTIER

THE JOURNAL FOR SPACE AND CYBERSPACE PROFESSIONALS

SCHRIEVER WARGAME 2010

INSIDE:

Headquarters
Air Force
Space Command
Peterson Air Force Base, Colorado

Commander
General C. Robert Kehler

Vice Commander
Maj Gen Michael J. Basla

Director of Public Affairs
Col Dewey Ford

Creative Editor
Ms. Nadine Sage

High Frontier Staff

Mr. Steve Tindell
Dr. Rick Sturdevant
Maj Catherine Barrington
Maj Bradley Brewington
Maj Vanessa Hillman
Maj April Wimmer
Mr. Gregory V. Williams

Editorial content is edited, prepared, and provided by the *High Frontier* staff. All photographs are Air Force photographs unless otherwise indicated.

High Frontier, Air Force Space Command's space professional journal, is published quarterly. The journal provides a scholarly forum for professionals to exchange knowledge and ideas on space-related issues throughout the space community. The journal focuses primarily on Air Force and Department of Defense space programs; however, the *High Frontier* staff welcomes submissions from within the space community. Comments, inquiries, and article submissions should be sent to AFSPC.PAI@peterson.af.mil. They can also be mailed to:

AFSPC/PA
150 Vandenberg St. Ste 1105
Peterson AFB, CO 80914
Telephone: (719) 554-3731
Fax: (719) 554-6013

For more information on space professional development please visit:
http://www.afspc.af.mil

To subscribe:
Hard copy: nsage@sgis.com
Digital copy: http://www.af.mil/subscribe

Cover: Schriever Wargame 2010: US, Australia, Canada, and United Kingdom. Cover designed by Daniel Santistevan.
Back Cover: Blue binary code, digital background, psdGraphics.

HIGH FRONTIER

The Journal for Space and Cyberspace Professionals

November 2010 Volume 7, Number 1

Contents

Next Issue: ***Implications of the New National Space Policy***

National Security Fundamentals in the Space and Cyber Domains

Ambassador Lincoln P. Bloomfield, Jr.
Chairman, Stimson Center
Washington, DC

Schriever Wargame 2010 (SW 10) stimulated the participants' thinking on how the operational toolkit and authorities being developed or contemplated for US military commanders can best serve national security purposes in an unfolding crisis. Potent offensive or defensive capabilities, and accurate knowledge of an adversary's actions and their effects, are keys to tactical success. Being able to use those tools to deter war, or to manage and resolve a conflict at an acceptable cost in lives, treasure, and national reputation, is the strategic measure of success. Following are some policy-level insights gained from the exercise.

From Marquis of Queensberry Rules to the Law of the Jungle

Picture the White House Situation Room a generation ago at the height of an escalating crisis between the US and a major nuclear-armed adversary. The president has directed a series of specific actions to position our strategic nuclear forces for higher alert; the secretary of defense, joined by the chairman of the Joint Chiefs of Staff, has conveyed the president's directions to the commander of US Strategic Command (STRATCOM), who will implement them. US nuclear policy experts, analysts, and planners have long since developed courses of action to maintain crisis control and prevail at every level of escalation, their certitude based on the existence of nuclear plans, policies, and procedures in the adversary camp. Thousands of miles away, the adversary's senior civilian and military leaders undertake a similar process as the geopolitical conflict between the US and its nuclear rival is played out.

Back in the situation room, a US advisor with deep expertise on the adversary's nuclear doctrine and posture is describing the adversary's actions for the president and the assembled national security senior leadership. The advisor refers to intelligence and warning indicators that both the US and its adversary understand to be departures from normal readiness conditions, some of these codified in bilateral arms control agreements as a way of maintaining strategic stability. "Look at what they haven't done," the US advisor explains. "They have not flushed their bombers or boomers (nuclear weapons-capable submarines); key airfields and facility parking lots are no busier than usual; and certain leadership figures remain on travel around the country or overseas, and do not appear to have been recalled to the capital." With the benefit of such context—weighing what has occurred against what would be expected to occur in a more aggressive scenario—the US president is able to tailor the US response so as to assert US interests and, at the same time, avoid escalating the crisis and risking catastrophic consequences.

Now, jump ahead to a future 21st century scene in the White House Situation Room as a crisis breaks out with a powerful adversary known to have sophisticated offensive capabilities in the space and cyber domains. Reports are coming in about anomalies affecting the supervisory control and data acquisition systems that run certain power, telecom, and transportation networks within the US. Benefiting from upgraded space situational awareness capabilities, STRATCOM is reporting a space event involving the sudden failure of systems on one or more militarily important US satellites, effects which it is able to attribute with strong circumstantial evidence if not absolute certainty, to actions by the adversary.

Security advisors, in the new space and cyber age as in the longstanding nuclear age, are able to compose for the president a compelling all-source summary of these apparent hostile acts against the US. However, in contrast to the nuclear standoff of an earlier era, there are no bilateral negotiations between Washington and the adversary government aimed at maintaining crisis stability—nothing to curb the dangers of hostilities in space or destructive actions against the information systems on which the civil and military sectors of each country has come to depend. The good news is that there has never been a destructive conflict waged in either the space or cyber domains. The bad news is that no one around the situation room table can cite any history from previous wars, or common bilateral understandings with the adversary, relating to space and cyber conflict as a guide to what the incoming reports mean, and what may or may not happen next.

This is the big difference between the space-cyber domains, and the nuclear domain. There is, in this future scenario, no credible basis for anyone around the president to attribute restraint to the adversary, no track record from which to interpret the actions by the adversary. There is no crisis management history: the president has no bilateral understandings or guide-

There is, in this future scenario, no credible basis for anyone around the president to attribute restraint to the adversary, no track record from which to interpret the actions by the adversary.

So long as we live in a world where no country including the US has well-documented experience with either war in space or 'cyber conflict' with an adversary, the potential for error, misunderstanding, miscalculation, overreaction, and escalation will remain high.

lines from past diplomatic discussions, and no operational protocols from previous incidents where space and cyber moves and counter-moves created precedents. Perhaps the adversary intended to make a point with one series of limited attacks, and hoped for talks with Washington and a compromise; but for all the president knows, sitting in the situation room, the hostile actions taken against America's space assets and information systems are nothing less than early stages of an all-out assault on US interests.

In 2009, at the Schriever V Wargame, players had discussed the potential utility of internationally agreed protocols and confidence building measures such as a Space Code of Conduct.[1] However, at that time the general perception among the assembled military and defense experts was that any proposition to trade away freedom of action in space as the price of an international arms control agreement was at best a questionable bargain for the US. Particularly given that in a future confrontation, the US could not trust its adversary to live up to its obligations in an arms control agreement, the advantage of such a trade was not apparent.

The SW 10 exercise changed that perception precisely because tactical freedom of action was not the only asset worth having in a future crisis. Equally important was having some basis to judge the intent and aims of the adversary. If left only to interpret operational reports from military commanders—or, in the case of cyber networks, incident reports from state and local authorities, and industry—about anomalies and disruptions that are reasonably attributable to the deliberate actions of an adversary, a future president has but one conclusion to draw: the US is under attack. If war, as Clausewitz said, is the continuation of politics by other means, space and cyber war with no precedent or protocols emerged in the SW 10 exercise as a highly problematic channel through which to prosecute "politics," and thereby serve the national interest, in a crisis.

One take-away, therefore, is the advisability of exploring specific protocols and norms relating to possible military actions in the space and cyber domains. While proposals already exist for a space Code of Conduct, the US warfighting community would do well to examine potential protocols in detail to identify those that conform to its mission objectives. The Schriever franchise is well suited to the task. Absent specific norms for space-cyber conflict, our political leaders will likely be compelled to "talk" as they "shoot"—communicating very plainly their aims and intentions. Otherwise, not knowing what the US intends, the adversary may well anticipate the worst and act accordingly. While adversaries in wartime will be very slow to believe each other's words, this is a lesser concern than leaving it to the adversary to figure out American intentions.

Related to this is the possibility that the adversary's sites or systems targeted by the US may have different or secondary purposes than those presumed by US intelligence. These alternative purposes may be deemed far more vital and strategic than the US side had thought—a misunderstanding that could immediately escalate the conflict. There is no assurance that clear messaging at the leadership level between the US and the adversary would serve as a brake on escalation in such a situation; but the absence of such communication would leave each side with no incentive or excuse for restraint. So long as we live in a world where no country including the US has well-documented experience with either war in space or 'cyber conflict' with an adversary, the potential for error, misunderstanding, miscalculation, overreaction, and escalation will remain high.

Figure 1. Brig Gen Robert J. Chekan and Ambassador Lincoln P. Bloomfield, Jr. at Senior Leadership Seminar in Washington, DC for Schriever Wargame 2010.

Offensive Measures with Unpredictable Effects in Domains Without Boundaries

The nature of both space-based and terrestrial information systems raise new challenges for the US and its allies in preserving the peace and defending their shared interests if threatened. Space assets are costly and scarce; dependent on terrestrial facilities, they may fail if disruption occurs at a single node anywhere in the system.[2] Because space systems are both costly and (for most countries) scarce, they may carry secondary and tertiary functions, servicing government or private sector interests. The US may have imperfect knowledge of what purposes and end-users are served by a foreign space system. Taking deliberate offensive action to disrupt or disable a foreign system, therefore, can bring unpredicted and unintended consequences, even when it achieves the first-order tactical purpose of degrading a known military capability relevant to the adversary's prosecution of the conflict.

Terrestrial information systems, unlike space systems, may be robust, redundant, and defended. While space systems are comparatively scarce, costly, and vulnerable, terrestrial information networks are widespread and constantly proliferating, becoming ever more accessible to the world's population and enabling ever more aspects of daily life. The result is the same: these cyber-networks not only support military capabilities, but they serve multiple users and end-uses. If intelligence analysts and military planners are less than certain of what uses and end-users are tied to a particular foreign satellite or space system, they are surely far less able to predict the second, third, and fourth-order effects of disrupting a foreign cyber network.

Two liabilities emerge from the prospect of defending national interests militarily in the space and cyber domains. The first, mentioned above, is the possibility of targeting an adversary asset with one known purpose, only to find that it has far more sensitive purposes and becomes a trigger for unintended escalation of the conflict. The second is that the physics of space and cyber systems frustrate the military planner's ethical quest for 'surgical' strikes: by the very nature of these geographically unbounded systems and their capacity to serve multiple purposes, as military targets they carry high risks of collateral damage. Moreover, unlike probably any circumstance yet encountered in conventional warfare, with space and cyber systems the negative collateral impacts could be located anywhere, and harm anyone; the unintended damage incurred could exceed the importance of the tactical objective. Most challenging of all, the president and US military commanders would likely have little if any ability to predict who, where, and how collateral effects will impact, or the severity of the harm.

In a world where governments are finding their sensitive activities ever more vulnerable to public exposure and scrutiny, the US should expect, and plan, to be held accountable for all of the impacts caused by its use of military force, including technological tools suited to the space and cyber domains. The moral and ethical heritage underpinning US security policy that gave rise, in recent decades, to the exhaustive preparation of "no-strike" lists in advance of major combat operations such as the removal of Saddam Hussein's regime in Baghdad in 2003, do not cease to exist when geopolitical conflict migrates into the space and cyber domains. The task for US security policy is to conform operational concepts to a world increasingly dependent on these new, geographically unbounded systems, so that no adversary can gain undue advantage by degrading or holding them at risk.

Early Insights on Space Allies: the Good News

In at least one important aspect, this exercise reflected the clear direction of the 2010 Quadrennial Defense Review and National Security Strategy: certain allies participated as full stakeholders. No information was denied to them; their national assets were combined with US systems; and presidential decisions were deliberated in their presence, with the benefit of their counsel.

Traditional benefits to US security from alliances have included the geographic access they afford to areas of possible conflict; deterrence derived from multinational solidarity; and sharing of burdens among multiple armed forces and national budgets. As significant as these advantages are, in the post-Cold War era there has been a fractured US consensus on the subject of alliances, with a school of thought questioning whether the US may at times be better off acting unilaterally and preserving maximum political-military freedom of action. When allies do not substantially encumber US policy decisions, when their presence in the battlespace adds materially to the conduct of the mission through compatible (if not identical) rules of engagement and a level of self-support that does not require a significant diversion of US resources, the political and military benefits can be substantial.

Based on the SW 10 wargaming experience, in a conflict potentially involving space and cyber networks, the US appears to gain more than it gives up by making common cause with close allies. Here are five prospective benefits of such alliance relationships:

1. Allies have assets such as satellites and ground stations providing communications and intelligence. An adversary hoping to compel the US to concede to its demands by threatening US space assets will have reduced grounds for optimism if allied systems are also functioning and available to support the US side in the confrontation. This enlarged network of space systems creates a measure of deterrence.

2. Allies have geopolitical standing and interests of their own. An adversary hoping to isolate the US in a confrontation will be frustrated by the realization that the price of escalating to hostilities against the US in space is likely

An adversary hoping to compel the US to concede to its demands by threatening US space assets will have reduced grounds for optimism if allied systems are also functioning and available to support the US side in the confrontation.

Just as public disagreement with our allies might invite adventurism by an adversary, political and legal solidarity between the US and its allies can contribute to deterrence.

to be a state of belligerency with additional governments and trading partners. This expanded political and economic profile on the US side similarly creates deterrence.

3. Allies have tactical value-added based on their own competencies. Having allied teammates who can bring to the table separate intelligence information, analytical perspectives, planning concepts, and specialized language and technical skills can enrich the quality of the options available to US decision makers and field commanders. This enhanced operational capability, if appreciated by the adversary, affords a further increment of deterrence.

4. Allies have their own national policies and interpretations of international laws and norms. This aspect of alliance management has sometimes been perceived in the US as an inconvenience or even a liability. However, a lesson of recent history for civilian policy makers is that in making the decision to use military force, the US will do well not only to assert the legitimacy and legality of its actions, but to make a case that is credible to and accepted by other countries, allies above all. By including close allies in the deliberative process aimed at maintaining the security of space and cyber systems against hostile threats, US decision makers can forestall dissension among friendly capitals once military action is taken, and hopefully receive strong public backing from allied governments. Just as public disagreement with our allies might invite adventurism by an adversary, political and legal solidarity between the US and its allies can contribute to deterrence.

5. Finally, allies have authorities that may prove useful to the war effort. Government activities in the space and (particularly) cyber arenas have the potential to intersect with fundamental American rights involving privacy and private property. Allied legal systems and government policies, while similar to the US are not identical, and allied governments may have authorities relevant to countering these new threats that US officials do not have. In such instances, of course, US officials can have no involvement of any kind with an action by a foreign government that would not be permissible under US law. However, allied governments are free, indeed expected, to protect their national interests according to their own laws. Separate but sympathetic action by allies in facing a threat to shared interests is yet another potential advantage of alliance relationships contributing to space and cyber security, and thus deterrence.

As the US deepens its national security dependence on space and cyber systems, potential adversaries continue to press ahead with the development of capabilities to hold these systems at risk. The Schriever wargaming franchise, by simulating future space and cyber conflict, is helping civilian and military practitioners to recognize what tools, procedures, and thought processes from the past may be relevant to securing our interests in these new domains. More importantly, it is offering a glimpse at challenges of future conflict that are most likely to require fresh thinking and new solutions.

Notes:

[1] See, for example, work on space security being conducted at the Henry L. Stimson Center in Washington, http://www.stimson.org/space/programhome.cfm.

[2] The author credits fellow SW 10 participant Lt Gen (USAF, retired) Robert Elder, for the useful insight that the term "circuit" may better describe the functioning of a space system than "network" which implies robustness that may not exist.

Ambassador Lincoln P. Bloomfield, Jr. (Harvard, a.b, cum laude, Government, 1974; Fletcher School, M.A.L.D., 1980) is chairman of the Henry L. Stimson Center in Washington, DC. He was the president's special envoy for Man-Portable Air Defense System Threat Reduction from 2008-09, and assistant secretary of state for political military affairs as well as special representative of the president and secretary of state for Humanitarian Mine Action from 2001-2005. He previously served as deputy assistant secretary of state for Near Eastern Affairs (1992-93), deputy assistant to the vice president for National Security Affairs (1991-02), member, US Delegation to Philippine Bases Negotiations (1990-91), member, US Water Mediation in the Middle East (1989-90), and principal deputy assistant secretary of defense for International Security Affairs (1988-89), among other positions in the Department of Defense (OSD/ISA) beginning in 1981. He is president of Palmer Coates LLC, senior advisor at Akin Gump Strauss Hauer & Feld LLP, operating advisor at Pegasus Capital Advisors L. P., senior advisor at ZeroBase Energy LLC, and chairman of the board of Bell Pottinger Communications USA LLC.

We are interested in what you think of the ***High Frontier*** Journal, and request your feedback. We want to make this a useful product to each and every one of you, as we move forward to professionally develop Air Force Space Command's space and cyberspace workforce and stimulate thought across the broader National Space Enterprise. Please send your comments, inquiries, and article submissions to: HQ AFSPC/PA, *High Frontier* Journal, 150 Vandenberg St, Suite 1105, Peterson AFB, CO 80914-4020, Telephone: (719) 554-3731, Fax: (719) 554-6013, Email: afspc.pai@peterson.af.mil, To subscribe: hard copy, nsage@sgis.com or digital copy, http://www.af.mil/subscribe.

U.S. AIR FORCE

AIR FORCE SPACE COMMAND

AFSPC/PAI
150 Vandenberg St.
Ste 1105
Peterson AFB, CO 80914
Telephone: (719) 554-3731
Fax: (719) 554-6013

For more information on space professional development visit:
www.peterson.af.mil/spacepro

Air & Space Power Journal:
www.airpower.maxwell.af.mil/airchronicles/apje.html