Achieving a Credible Nuclear Deterrent

Lt Col Samuel L. McNiel, USAF*

Imagine trying to keep a 1957 Chevy running in pristine condition—perhaps not difficult for a classic-car aficionado, but such a vehicle would not be practical for daily commuting. Gen Kevin Chilton, commander of US Strategic Command, points out that the B-61 warhead, designed in the 1950s but still in the US nuclear arsenal, contains vacuum tubes—something he equates to maintaining a '57 Chevy for everyday use.[1]

A credible deterrent requires adversaries to believe that (1) the instrument of deterrence will deliver the level of destruction claimed and (2) the entity wielding the instrument would actually employ it. The absence of either belief destroys the deterrent's credibility. Over the past two decades, both the reliability of US nuclear weapons and certainty about US political will to employ them have declined; therefore, the credibility of US deterrence, ultimately guaranteed by nuclear weapons, has also declined. Furthermore, the United States no longer maintains a sufficient industrial base for these devices—the nuclear weapons complex—to support its nuclear deterrence strategy. This article argues that America should restore the credibility of its nuclear deterrence by designing, testing, producing, and fielding a new nuclear weapon, which would effectively revive a viable nuclear weapons complex and demonstrate political resolve.

After offering a brief background on nuclear weapons and the weapons complex, this article examines the foundational nature of nuclear weapons with regard to deterrence strategy, our neglect of the nuclear weapons complex, the uncertain reliability of the weapons stockpile, and, consequently, the diminished credibility of our deterrence. It concludes by showing that designing and fielding a new weapon will correct these deficiencies and provide new military capabilities.

Nuclear Weapons and the Complex

A basic understanding of nuclear weapons—very complex mechanisms made up of thousands of parts—will help inform a discussion of their industrial base.[2] At the heart of a nuclear weapon resides the nuclear explosive package (NEP). All current US weapons consist of two stages. The first stage, or primary, works on the same principle as the atomic bombs employed during World War II. At the center of the primary lies a "pit," a hollow core of fissile material (usually plutonium) surrounded by a chemical explosive. When the explosives detonate, the resulting shockwave compresses the pit, which becomes so dense that it creates a runaway nuclear fission reaction. Before the pending nuclear explosion destroys the pit, a "boost gas" (a mixture of deuterium and tritium) is injected into the pit to increase the fraction of plutonium that undergoes fission, yielding greater energy

*A space and missile operations officer, the author currently attends the Industrial College of the Armed Forces at National Defense University.

for use in the second stage. The harnessed portion of the primary's energy then ignites the second stage's fusion fuel. Most of the energy yield from thermonuclear weapons comes from the secondary.[3] A *nuclear warhead* includes the NEP along with supporting components.[4]

A *nuclear weapon*, composed of a nuclear warhead and a set of supporting nonnuclear components, produces nuclear energy of a militarily significant yield.[5] The components consist of weapon-specific items such as fuses, batteries, and reentry vehicles and bodies.[6] All nine nuclear weapon types currently in the US stockpile were designed in the last century—some as far back as the 1950s but none more recently than the 1980s.[7]

Eight government-owned, contractor-operated sites make up the nuclear weapons complex:

> Los Alamos National Laboratory . . . and Lawrence Livermore National Laboratory . . . which design [NEPs]; Sandia National Laboratories . . . which designs nonnuclear components; Y-12 Plant . . . which produces uranium components and secondaries; Kansas City Plant . . . which produces many of the nonnuclear components; Savannah River Site . . . which processes tritium from stockpiled weapons to remove decay products; Pantex Plant . . . which assembles and disassembles nuclear weapons; and the Nevada Test Site, which used to conduct nuclear tests but now conducts other weapons-related experiments that do not produce a nuclear yield.[8]

Nuclear Weapons Strategy Remains Relevant

A credible deterrence, impossible without reliable nuclear weapons, advances US interests in three ways: (1) underpinning US national security by guaranteeing the US military's ability to bring overwhelming force to bear against an adversary, (2) helping prevent the proliferation of nuclear weapons by removing the imperative for allies to develop their own nuclear weapons, and (3) dissuading rivals from breaking treaties designed to control nuclear weapons and then engaging in an arms race. According to the Congressional Commission on the Strategic Posture of the United States, "In a basic sense, the principal function of nuclear weapons has not changed in decades: deterrence. The United States has the weapons in order to create the conditions in which they are never used."[9]

Nuclear weapons remain a critical underpinning of US national security and defense strategy, as noted Pres. Barack Obama, speaking in Prague in April 2009: "Make no mistake: As long as these [nuclear] weapons exist, the United States will maintain a safe, secure and effective arsenal to deter any adversary, and guarantee that defense to our allies."[10] The *Capstone Concept for Joint Operations* further amplifies this theme, observing that US forces once again need to make strategic nuclear deterrence a focus area and that US failure to maintain its nuclear capabilities could encourage potential adversaries.[11] With regard to the role of fielded forces, General Chilton said that the nuclear mission remains US Strategic Command's top priority, voicing his belief in the importance of maintaining a safe, reliable nuclear stockpile until nuclear weapons are no longer a part of the country's arsenal.[12]

In addition to the classic deterrence goal of preventing a massive nuclear attack against the United States, today's nuclear arsenal "should be designed to provide robust deterrence in the most difficult of plausible circumstances: during conventional war against a nuclear-armed adversary."[13] Without an ability to back up threats with force, deterrence is not credible. Ensuring the availability of nuclear capabilities that are militarily useful for all situations does not make the United States more likely to use nuclear weapons; instead, it gives credibility to US deterrence.[14] To remain an effective deterrent against lesser nuclear powers, especially during conventional conflict with a nuclear-armed enemy, the US nuclear arsenal should give the president options having the greatest probability of

destroying an adversary's nuclear forces without causing excessive casualties—a requirement that may call for new, low-yield weapons. Moreover, Keir Lieber and Daryl Press write that "any nuclear arsenal should also give U.S. leaders options they can stomach employing in these high-risk crises. Without credible and effective options for responding to attacks on allies or U.S. forces, the United States will have difficulty deterring such attacks. Unless the United States maintains potent counterforce capabilities, U.S. adversaries may conclude—perhaps correctly—that the United States strategic position abroad rests largely on a bluff."[15]

and the will to use it in defense of our allies. If our allies cannot depend on us, then they will be motivated to develop their own nuclear weapons and the means to deliver them. Most of them are capable of doing that in a few years."[18]

In addition to helping deter attacks against the United States and its allies and helping prevent nuclear proliferation, a credible nuclear deterrent also dissuades China and Russia from pursuing a nuclear arms race with the United States. As long as America can produce and field enough nuclear weapons to maintain strategic balance with Russia, that country has no incentive to break arms control agreements in an

Deterrence strategy is essential not only for helping to protect the United States from attack but also for assuring allies and partners.

Deterrence strategy is essential not only for helping to protect the United States from attack but also for assuring allies and partners. This assurance, stemming from a concept known as extended deterrence, eliminates the need for allies and partners without nuclear arms to pursue weapons programs of their own.[16] Many of those parties could launch successful programs and begin building their own nuclear arsenals within a few years if the United States fails to meet their deterrence needs, thus triggering global waves of nuclear proliferation contrary to US interests.[17] Gen John Loh, formerly the Air Force's vice chief of staff, clearly articulates the importance of extended deterrence: "Extended deterrence provides our umbrella of deterrence for others. . . . But that means we have to maintain a credible, robust nuclear force attempt to attain strategic supremacy. However, failure to do so could have a destabilizing effect, ignite a new nuclear arms race, and even tempt China to gain nuclear strategic balance with the United States.[19]

Atrophy of the Nuclear Weapons Complex

Any strategy that relies on nuclear weapons requires the existence of an industrial base—the nuclear weapons complex—capable of meeting the strategy's needs. Because the United States has underfunded and neglected its complex for two decades, the industrial base has atrophied to a point that, unless we take corrective action soon, we may lose the ability to maintain or produce nuclear weapons. If

that happens, we could regain it only through great expenditure of time and treasure. Melanie Kirkpatrick highlights the severity of the problem: "Since the end of the Cold War, the U.S. nuclear weapons program has suffered from neglect. Warheads are old. There's been no new warhead design since the 1980s, and the last time one was tested was 1992, when the U.S. unilaterally stopped testing."[20] Furthermore, the United States lacks the industrial capacity to manufacture nuclear weapons at production levels. True, it could produce a few by using laboratory assets, but that is not the same as serial production. Finally, only a handful of engineers and scientists still in the federal work force have designed and tested nuclear weapons—and all of them will retire in a few years.[21]

At the component level, the United States can no longer manufacture pits (the Rocky Flats plant, which produced pits, shut down in 1989) or produce tritium in weapons-complex facilities. In 2002 the congressionally mandated Panel to Assess the Reliability, Safety, and Security of the United States Nuclear Stockpile (the Foster Panel) said that the National Nuclear Security Administration (NNSA) had only mixed prospects of fulfilling its intended weapons refurbishments, including the B-61 and W-76 weapons, due in part to the inability to produce new pits.[22] Even though the NNSA declared in 2004 that "restoring our capability to manufacture plutonium pits is an essential element of America's nuclear defense policy," it delayed a decision to build a new pit-manufacturing facility, leaving the United States without production-level capability.[23] Critical to obtaining the designed yield, tritium has a decay rate of 5.5 percent per year, giving it the shortest shelf life of a nuclear weapon's components, but the US nuclear weapons complex has not produced it since 1988, when the K reactor at the Savannah River Site shut down. Tennessee Valley Authority reactors did resume production in 2005, however.[24]

Finally, the country is not producing top-level nuclear chemists to replenish the nuclear workforce. In the early 1960s, US universities granted up to 36 PhDs in nuclear chemistry each year, but that number has steadily declined.[25] The American Physical Society, the world's second-largest organization of physicists, commented that "only a handful of U.S. university chemistry departments currently have professors with active research programs in nuclear chemistry. . . . Thus, advanced education in nuclear chemistry education is all but extinct in the United States."[26]

The Obama administration's proposed budget for fiscal year (FY) 2011 includes $11.2 billion for the NNSA, a 13.4 percent increase from FY 2010's appropriation.[27] Thomas D'Agostino, NNSA administrator, said that more than $7 billion of the requested funds are for what NNSA terms weapons activities, which include increased investments to begin to recapitalize some physical infrastructure and build a resource base of human capital.[28] Although such a step is helpful, even the increase in funding for facilities will not allow the United States to reestablish the production level for pits. Further, it will not address the basic issue of uncertainty regarding the stockpile's reliability—an issue inherent in an approach that excludes full-scale testing of weapons. As the Foster Panel reports, even though no one can predict exactly when it will occur, "at some point, the nuclear test pedigree for a weapon will no longer be relevant."[29]

Weapons Reliability, Political Will, and Credible Deterrence

The Stockpile Stewardship Program (SSP) and Life Extension Program (LEP) may prove insufficient to ensure the reliability of stockpiled weapons—and any doubt is too much. The United States conducted 1,000 nuclear tests between 1945 and 1992.[30] Since self-imposing a moratorium on testing, the country has relied on the science-based SSP to certify the reliability of weap-

ons. That program, which "uses data from past nuclear tests, small-scale laboratory experiments, large-scale experimental facilities, examination of warheads, and the like to better understand nuclear weapon science," closely examines 11 stockpiled weapons of each type per year.[31]

If the SSP discovers problems with a warhead, then the LEP attempts to fix them by remanufacturing needed parts. Most experts agree that this practice has been sufficient to date and can probably continue for the short term, but they debate its viability in the long term. According to a report by the Lawrence Livermore National Laboratory in 1987, "Exact replication, especially of older systems, is impossible. . . . Documentation has never been sufficiently exact to ensure replication. . . . The most important aspect of any product certification is testing: it provides the data for valid certification."[32] In general, as the US nuclear arsenal matured through years of development, weapons became smaller and lighter so smaller delivery vehicles could carry them; thus, a single missile could carry more warheads, or a booster could carry warheads farther. This reduction in size required very exotic engineering, described by Ambassador Linton Brooks, former NNSA administrator, as "very close to performance cliffs."[33] Because of the need to make warheads as small and light as possible, yet assure that they would not accidentally detonate, even in very harsh environments, the designs included very little performance margin. In the absence of testing, Brooks feared that as the weapons aged beyond the time when engineers originally thought the warheads would be retired, the cumulative effect of changes from both the aging of the weapons and the utilization of remanufactured parts would induce increasing uncertainty about their reliability.[34]

In the case of the B-61 warhead, the LEP has gone beyond just attempting to replace original parts with similar new parts. It will try to change the B-61—essentially the only air-delivered weapon in the US arsenal—from utilizing analog circuitry to digital circuitry.[35] Under existing policies, this change—slated to take place by 2017—will occur without testing the complete nuclear weapon. Planning on untested weapons to deter existential threats to the country or expecting leaders of second-tier regional powers to believe that such weapons will always work as designed may be wishful thinking.

In addition to technical reliability, credible deterrence requires the political will to supply resources for nuclear weapons programs and to convince potential enemies that we have no compunctions about employing nuclear weapons if we must. The current administration and Congress are continuing the decades-long trend of allowing the credibility of US nuclear deterrence to erode. In his Prague speech, President Obama said,

> So today, I state clearly and with conviction America's commitment to seek the peace and security of a world without nuclear weapons.
>
> . . . First, the United States will take concrete steps towards a world without nuclear weapons. . . . We will reduce the role of nuclear weapons in our national security. . . .
>
> . . . My administration will immediately and aggressively pursue U.S. ratification of the Comprehensive Test Ban Treaty.
>
> And to cut off the building blocks needed for a bomb, the United States will seek a new treaty that verifiably ends the production of fissile materials intended for use in state nuclear weapons.[36]

Although administrations from across the political spectrum have endorsed the dream of a world without nuclear weapons, none in recent history have so overtly stated their intention to de-emphasize the role of these weapons in US national security.[37] Even though President Obama pledged to maintain a reliable nuclear-deterrent force, an adversary could interpret or misinterpret his position in a way that would raise doubt about US willingness to employ nuclear weapons under any circumstances, thus diminishing the credibility of US deterrence.

Through the power of the budget, Congress has also aided the demise of the nuclear weapons complex and diminished the credibility of the stockpile. In 2008 it cut off all funding for the Reliable Replacement Warhead (RRW) (formally terminated by the president in March 2009) and ensured that the NNSA did not proceed with its Complex 2030 program, which would have revitalized the nuclear weapons complex and positioned it to manufacture a new warhead.[38] Even if Congress approves the president's 2011 budget request to increase NNSA funding, improve some infrastructure, and refurbish Trident missile warheads and B-61 bombs, it has shown no willingness to commit strongly to nuclear deterrence by mandating design of a new warhead, ensuring production-level infrastructure, or directing new nuclear-yield testing of weapons.

The strongest political opposition to designing a new nuclear weapon or testing existing weapons comes from those who believe that engaging in design and test activities would increase the proliferation of weapons and weaken US credibility on nonproliferation. However, this position is inconsistent with historical events. Since the United States unilaterally stopped nuclear testing in 1992, France, China, India, Pakistan, and North Korea have tested nuclear weapons, three of those countries having conducted their first tests. Currently Iran is likely pursuing a nuclear weapons program. Libya, Syria, and Iraq had active programs, curtailed only after intensive military and political efforts. No evidence suggests that US restraint slowed other countries' determination to field nuclear weapons. Moreover, as previously discussed, if US allies no longer believe that America's doctrine of extended deterrence rests on reliable capabilities, they too may pursue nuclear weapons programs. The United States can best enhance its position on nonproliferation by not engaging in proliferation activities and holding accountable all who expand nuclear weapons technology. Designing and testing to maintain the US arsenal in no way extends nuclear weapons, but those activities do deter countries that might try to gain strategic equivalency with the United States or threaten the use of nuclear weapons to coerce it. Therefore, although well intended, the political opposition to maintaining strong, credible nuclear deterrence actually makes proliferation more likely.

If US allies no longer believe that America's doctrine of extended deterrence rests on reliable capabilities, they too may pursue nuclear weapons programs.

Recommendations

The United States should design, test, produce, and field a new nuclear weapon in order to maintain a viable nuclear weapons complex and ensure the credibility of the deterrent force. New technologies and materials allow for constructing a weapon with safer materials and antitampering technologies. Further, lower-yield weapons would add military utility and avoid unacceptable

levels of collateral damage. Additionally, a penetrating version could hold deeply buried targets at risk, obviating the need for high-yield weapons.

Before termination of the RRW program, Congress directed the NNSA to have the JASON advisory group, a prestigious organization of scientists who advise the government on defense matters, conduct an independent peer review of the need for the RRW.[39] According to that group, "To ensure the viability of its nuclear deterrent, the United States must initiate and invest in the RRW program now—so there will be no disconnect between today's credible deterrent and the one required for the future."[40]

The process of designing, testing, and producing a new weapon would revitalize the US industrial base for nuclear weapons, ensure that technical and intellectual capacity exists to validate the stockpile's reliability, and restore the credibility of US nuclear deterrence. Additionally, it would signal to friends and allies the United States' resolve to uphold its commitments to extended deterrence, thus assuring them they do not need to pursue their own nuclear weapons programs. Finally, the process will send a strong message to Russia and China that it is in their best interest to remain in the nuclear-weapons-control regimes and that they have nothing to gain by trying to attain nuclear supremacy over the United States. No technical reasons stand in the way of launching this program immediately—political desire and the will to do so are all we need.

Conclusion

Because of technological and fiscal realities, US deterrence depends upon nuclear weapons. Until we find a highly reliable way of defeating a nuclear attack on the United States and until advances in long-range strike enable a completely successful, disarming counterforce attack against any enemy's nuclear forces, America must rely on deterrence provided by robust nuclear capabilities. No other weapon systems offer the same level of assurance of US survival.

In a misguided attempt to create a safer world, the United States allowed its ability to support its nuclear deterrent strategy to atrophy, diminishing confidence in the reliability of the weapons stockpile and in the political will to use those weapons if necessary. Thus, the ensuing damage to the credibility of US nuclear deterrence increases, not decreases, the probability of using nuclear weapons. Designing, testing, and fielding a new nuclear weapon will both revitalize the US nuclear weapons complex and restore the credibility of America's deterrence. ✪

Fort Lesley J. McNair, Washington, DC

Notes

1. Melanie Kirkpatrick, "Sounding the Nuclear Alarm," *Wall Street Journal*, 22 November 2008, http://online.wsj.com/article/SB122731227702749413.html (accessed 24 April 2010).
2. Jonathan Medalia, *The Reliable Replacement Warhead Program: Background and Current Developments*, CRS Report RL 32929 (Washington, DC: Congressional Research Service, 27 July 2009), 4, http://opencrs.com/document/RL32929/2009-07-27/download/1013/ (accessed 24 April 2010).
3. Ibid., 45.
4. Government Accountability Office, "Nuclear Weapons: Annual Assessment of the Safety, Performance, and Reliability of the Nation's Stockpile," GAO-07-243R (Washington, DC: Government Accountability Office, 2 February 2007), 4, http://www.gao.gov/new.items/d07243r.pdf (accessed 27 April 2010).
5. Ibid.
6. Ibid.
7. Ibid.
8. Medalia, *Reliable Replacement Warhead Program*, 45.

9. William J. Perry et al., *America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States* (Washington, DC: United States Institute of Peace Press, 2009), 20, http://media.usip.org/reports/strat_posture_report.pdf, (accessed 24 April 2010).

10. "Remarks by President Barack Obama, Hradcany Square, Prague, Czech Republic," 5 April 2009, White House, Office of the Press Secretary, http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered/ (accessed 24 April 2010).

11. Department of Defense, *Capstone Concept for Joint Operations*, version 3.0 (Washington, DC: Department of Defense, 15 January 2009), 30–31, http://www.dtic.mil/futurejointwarfare/concepts/approved_ccjov3.pdf (accessed 24 April 2010).

12. MSgt Ben Gonzales, "STRATCOM Leader Charts Nuclear Path for American Military," Air Force News Agency, 23 September 2008, http://www.af.mil/news/story.asp?id=123116467 (accessed 27 April 2010).

13. Keir A. Lieber and Daryl G. Press, "The Nukes We Need: Preserving the American Deterrent," *Foreign Affairs* 88, no. 6 (November/December 2009): 41.

14. Ibid., 49.

15. Ibid., 51.

16. Perry et al., *America's Strategic Posture*, 20–21.

17. Ibid., 10.

18. John Michael Loh, "Ensure Nuclear Deterrence by Developing New Bomber," *Omaha World-Herald*, 7 December 2009, http://www.omaha.com/article/20091207/NEWS0802/712079997 (accessed 24 April 2010).

19. Perry et al., *America's Strategic Posture*, 21–22.

20. Kirkpatrick, "Sounding the Nuclear Alarm," 1.

21. Ibid., 2.

22. John S. Foster Jr., chairman, *FY 2001 Report of the Panel to Assess the Reliability, Safety, and Security of the United States Nuclear Stockpile* (Washington, DC: Government Printing Office, 15 March 2002), 4, http://www.fas.org/programs/ssp/nukes/testing/fosterpnlrpt01.pdf (accessed 27 April 2010).

23. National Nuclear Security Administration, "NNSA Delays Modern Pit Facility Environmental Impact Statement and Selection of a Preferred Location," 28 January 2004, http://nnsa.energy.gov/news/print/1516.htm (accessed 24 April 2010).

24. Pam Sohn, "TVA Argues for Tritium Production at Sequoyah," *Chattanooga Times Free Press*, 4 February 2010, http://www.timesfreepress.com/news/2010/feb/04/tva-argues-for-tritium-production-at-sequoyah/ (accessed 27 April 2010).

25. American Physical Society Panel on Public Affairs Committee on Energy and Environment, *Readiness of the U.S. Nuclear Workforce for 21st Century Challenges*, June 2008, 12, http://www.aps.org/policy/reports/popa-reports/upload/Nuclear-Readiness-Report-FINAL-2.pdf (accessed 24 April 2010).

26. Ibid.

27. Walter Pincus, "Obama Budget Seeks 13.4 Percent Increase for National Nuclear Security Administration," *Washington Post*, 3 February 2010, A3, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/02/AR2010020203884.html (accessed 27 April 2010).

28. Senate Appropriations Subcommittee on Energy and Water Development, *Hearing on President Obama's Fiscal 2011 Budget Request for the National Nuclear Security Administration*, 111th Cong., 2nd sess., 10 March 2010.

29. Foster, *FY 2001 Report of the Panel*, 2.

30. Medalia, *Reliable Replacement Warhead Program*, 12.

31. Ibid., 7.

32. Ibid., 6.

33. Ibid., 5.

34. Ibid. The details lie beyond the scope of this article, but some observers support placing a high level of confidence in the SSP. In general, those who support the assessments believe that because of the quantity of past test data, advances in modeling and simulation techniques, and huge strides in high-powered computing, we now have sufficient understanding to accurately model all the effects of aging on weapons.

35. Senate Appropriations Subcommittee on Energy and Water Development, *Hearing on President Obama's Fiscal 2011 Budget Request*.

36. "Remarks by President Barack Obama."

37. Ibid.

38. Medalia, *Reliable Replacement Warhead Program*, 1.

39. Ibid., 2.

40. Ibid., 3. In an exchange between Senator Dianne Feinstein and Administrator D'Agostino during a hearing before the Senate Appropriations Subcommittee on Energy and Water Development on the president's NNSA 2011 budget request on 10 March 2010, Mr. D'Agostino acknowledged that in 2009 the JASON group said it believed that the life of existing nuclear weapons could be extended well into the future. However, he also pointed out that "in many cases we can't make things the way we used to make them 30, 40 years ago. We just don't have the people. We don't have the processing techniques." See Senate Appropriations Subcommittee on Energy and Water Development, *Hearing on President Obama's Fiscal 2011 Budget Request*.

It's Time to Fight Back

"Operationalizing" Network Defense

Mr. Nicolas Adam Fraser
Lt Col Robert J. Kaufman III, USAF, Retired
Lt Col Mark R. Rydell, USAF, Retired*

The Air Force's decision to stand up Twenty-fourth Air Force under Air Force Space Command creates an opportunity to scrutinize existing network warfare constructs with the goal of ensuring that network warfare operations carry out the Air Force's stated mission: "to fly, fight, and win . . . in air, space, and cyberspace."[1] Such a sweeping review would involve a significant number of organizations inside and outside the Air Force, encompassing discussions of policy, funding priorities, personnel, and cross-service coordination, to name a few. This article does not attempt to address all of the complex issues surrounding cyberspace operations; rather, it examines the most visible component of cyberspace warfare—network defense (NetD).

Since 1992 the Air Force has monitored its networks and responded to malicious network events. As the service has matured its ability to command and control its networks, some operational principles have unintentionally blended NetD and network operations (NetOps). This article proposes new operational constructs that will force a healthy distinction between network warfare—particularly NetD—and NetOps. Cyber targeting, the first proposed construct, emphasizes the need to proactively find, fix, track, and target an adversary. Cyber targeting operations can ensure that mission-critical systems or even network paths remain free of adversaries. The second construct, cyber engagement, is a collection of responses specifically designed to affect an identified intruder. Current NetD constructs and cyber targeting enable cyber engagement operations. Finally, we must closely coordinate both targeting and engagement operations with combatant commands (COCOM) and other national agency operations. Both cyber targeting and cyber engagement induce a robust contrast between maintenance of the network and defense of the network. Making such a distinction and employing the proposed constructs should result in more effective NetD operations.

Setting the Stage for Change

The Air Force has been discriminating in its definitions of NetOps and NetD, the former providing "effective, efficient, secure, and reliable information network services used in critical Department of Defense (DOD) and Air Force communications and information processes" and the latter "employ[ing] . . . network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt,

*All three authors work at the 688th Information Operations Wing at Lackland AFB, Texas, Mr. Fraser as chief of the Network Access Engineering Branch, Lieutenant Colonel Kaufman as deputy director of the 318th Information Operations Group, and Lieutenant Colonel Rydell as a senior associate with Booz, Allen, and Hamilton. All served tours on the Air Force Computer Emergency Response Team.

or usurp it. NetD can be viewed as planning, directing, and executing actions to prevent unauthorized activity in defense of Air Force information systems and networks and for planning, directing, and executing responses to recover from unauthorized activity should it occur."[2] The fact that the joint community does not have a term to describe what the Air Force calls NetOps means that it considers NetOps either a subset of NetD or simply a maintenance function that does not warrant discussion in a joint doctrine publication.[3] Due to the differences in joint and Air Force doctrine, we suggest simplified versions of NetD and NetOps so that the reader can immediately recognize each operation's responsibilities and priorities:

- network warfare operations / NetD: operations that seek to produce desired effects against an adversary tactically, operationally, and strategically. These operations, which require planning and intelligence support, can be reactive or proactive. Most importantly, NetD operations consider the discovery of an adversary not just a threat but an opportunity for operational engagement.
- NetOps: operations in which the maintainer primarily *acts upon the network* to provide reliable and secure network services. In reality an adversary who disrupts operations is no worse than a hardware failure since the goal involves maintaining availability and performance requirements. Just as we can replace hardware, so can we rebuild a compromised computer.

We contend that the Air Force does not actually conduct NetD operations as defined above. We support this claim by examining two principles that lie at the core of the service's current approach to NetD and that keep the Air Force reactive, thus weakening its ability to defend the network effectively.

Principle 1: Detecting the Adversary Is Paramount

This principle, the foundation upon which we have built most traditional NetD, consumes the bulk of the Air Force's NetD resources. The service relies on real-time monitoring and emphasizes hardened network perimeters to detect enemy activity. However, its motivation for doing so is of great importance. The Air Force wishes to detect the intruder or attacker, not to take action against him but to find and fix a security problem. The situation is analogous to how a security forces member on flightline patrol responds to a suspicious event. Upon seeing an intruder enter through a hole in the fence, he or she shines his flashlight on the hole and begins to fix it instead of following and capturing the intruder. Currently the Air Force makes no distinction between sophisticated and nonsophisticated intrusions, treating all breaches equally and responding in a way that protects and reestablishes the health of the network. It does not focus on assuring that we can perform required missions and continue NetOps despite adversary attacks.

Though important, detecting the adversary is not the only way to protect a network. Rapidly and regularly changing its configuration would also offer protection and would not require detection of the adversary to produce results.[4] Additionally, we do not advocate the end of detection efforts, something critical to NetD operations as we define it, but the motivation behind detection efforts must change. Finally, we concede that our best perimeter defenses and patch-management methodologies fail to deter or hinder sophisticated adversaries.[5] Although these methodologies are useful, we must supplement our current approach with one committed to achieving effects against the adversary and assuring mission success.

Principle 2: NetD Operations Are Successful When a Compromised Computer Is No Longer Compromised

This principle relegates NetD operations to a maintenance role within the Air Force, emphasizing network health at the expense of determining the enemy's effect on ongoing or future missions. Furthermore, we rarely use a compromised computer to engage the adversary. In addition to finding, analyzing, and fixing compromised computers, NetD operators must contest the adversary, even on our own networks, conceiving of and executing defensive strategies that affect him while assuring the integrity of priority war-fighting missions.

Because of this principle, probably more than its companion, we should really define the current NetD as NetOps. When an intrusion occurs and we open an "incident," when do we close it? Not when an operation concludes but when we consider the computer free of intruders and allow it to rejoin the network. Is that success? No. We should measure success by combat effectiveness; consequently, we must take measurements at the strategic, operational, and tactical levels to determine if we are attaining NetD objectives such as deterring the adversary from establishing or employing offensive capabilities against US interests.[6]

A New Construct

We propose correcting these problems by establishing operational units (of yet undetermined sizes) charged with truly affecting adversary operations that target Air Force and DOD networks. True, units in Twenty-fourth Air Force (including the 688th Information Operations Wing and the 67th Network Warfare Wing) are responsible for executing the Air Force's cyber mission; however, no units within Twenty-fourth Air Force now do what we suggest below. Our new paradigms will require reshaping existing units and, possibly, creating new ones.

The first proposed organization would have the inwardly focused mission of seeking out the adversary on Air Force and DOD networks. The second would have the outwardly focused mission of engaging him on those networks. Although both would work closely together (and with the established, continuous network-monitoring mission), they would be set apart by their commitment to planned missions or "sorties" linked to a commander's operational needs and terminated upon completion of the mission. At strategic levels, proper policies need to endorse proactive NetD strategies such as targeting and engagement. Next, at the operational level, we must develop plans to address specific adversaries and prescribe approved courses of action that allow network defenders to realize unity of effort, mass, surprise, and timeliness in cyberspace. Finally, at the tactical level, we must train and certify operators on NetD weapons that can compromise attacks or thwart attempts to gain access to Air Force networks. These organizations and plans will allow the Air Force to perform NetD operations that seek, engage, and act upon adversaries in cyberspace.

Cyber Targeting

Clearly, enemies—specifically advanced, persistent ones—reside within the Air Force network. Spearfishing attacks, which persuade users either to open a malicious attachment or click on a link to a malicious Web page, breach perimeter defenses without difficulty. The ease with which an adversary can gain access to DOD networks is outdone only by the ease with which he can navigate and maneuver after establishing "beachheads" within Air Force and DOD networks, both of which actions offer entry to high-value information or systems. A proactive approach, cyber targeting can identify intruders on our networks by using state-of-the-art NetD "weapons" not permanently located on the Air Force network, along with typical perimeter-security tools. We would conduct operations with a specific objective in mind, find the adversary, and then influence, disrupt,

or otherwise affect him. An operation would not terminate until we have identified the adversary and subsequently verified his absence, regardless of the terminating factor. These operations also demand proper planning and execution because of the tremendous amount of legitimate data in cyberspace, within which the adversary hides to do his work.

Cyber Engagement

Defense has always involved delaying, disrupting, deterring, or denying enemy objectives. However, if we assume the impossibility of completely stopping the adversary, then we must consider ways to significantly hinder or exploit his efforts. (By "exploit," we mean achieve second- and third-order effects on his decision-making capacity.) Cyber engagement makes the conscious decision to use DOD networks as a path to the adversary—a path for fulfilling defensive goals.[7] Upon discovering a compromised computer or network, NetD operators no longer would simply rebuild the system but would use intelligence and perhaps other NetD weapons to identify the intruder. Next, depending on the level of attribution and existing operation plans (OPLAN), they would conduct tactical operations against the adversary, utilizing the compromised computer or network as a launching point.[8] For example, during an operation, the NetD operator could intentionally pass inaccurate information to the enemy or manipulate exfiltrated data, rendering it untrustworthy. Regardless of the technique employed, the operator would always try to introduce unreliability, make intrusions more costly, or influence the adversary's actions. Consequently, operators must plan and coordinate these "response actions" with larger COCOM or national-level strategies.[9] Additionally, they must deconflict these kinds of operations from the day-to-day monitoring of network sensors.

As discussed above, cyber engagement covers a spectrum of operations, not simply network attack. Engagement assumes the inability of detection and protection efforts to defend the network properly. Instead it takes a different approach, one not limited to selection of a particular technology but concerned with actions necessary to meet defensive goals. To illustrate, during a football game, the offensive players attempt to reach the end zone, but the defense tries to stop them. Football defenses attempt to keep the opposing team out of the end zone not only by employing defense in depth (fielding a strong defensive line, linebackers, and safeties) but also by using different schemes to confuse the quarterback. For example, one linebacker might rush the quarterback while two others drop back in coverage—or the defensive coordinator might call for an all-out blitz. Regardless of the scheme, good coaches know they cannot always prevent the offense from scoring, but they can make its task difficult by confusing the opposing players, especially the quarterback.

With one eye on this analogy, we would have to say that the DOD currently plays defense without ever thinking about causing confusion amongst the offense. We don't have different defensive schemes, nor do we prepare plans for affecting the planning, execution, and, ultimately, the outcome of an encounter with the enemy. Instead our defense stands at the network perimeter, and we hope no one gets by undetected.

Cyber targeting and cyber engagement represent a significant paradigm shift in the way we conduct NetD operations. By factoring in the objectives of focused OPLANs, we can make NetD a stronger form of fighting than network attack.[10] Indeed, the US Army has already noted this in more traditional defensive operations.[11] Furthermore, NetD can take a more active role in network warfare while creating a much-needed distinction between itself and NetOps. Finally, these new constructs support the president's desire to go beyond criminal prosecution in responding appropriately to cyber attacks.[12]

A Simple Proposal

Planning and preparing for large-scale military operations, such as the invasion of Iraq in 2003, require that COCOM OPLANs be routed through each military service's lead NetD organization, thereby allowing network defenders to implement measures against enemy targeting of DOD networks and prevent any disruption of the OPLAN's execution. Requirements provided by the COCOMs usually address generic threats. When operations commence, we usually take proactive steps such as blocking the addresses of hostile Internet protocols.

In these traditional situations, we treat the networks as a support element. That is, our networks need to function without disruption in order for our symmetric warfare capabilities to operate—analogous to saying that the fuel trucks need to function so the F-16s can take off. It is difficult to contemplate fighting on US networks, but NetD operations must take advantage of access to enemy NetOps and respond by decreasing the credibility of stolen information, increasing the cost of an attack on Air Force and DOD networks, or allowing the United States to influence the adversary's perceptions prior to and during all phases of conflict.

We propose the following as a way of highlighting the utility of this new construct, which truly thinks of NetD as a form of asymmetric warfare. Currently, each OPLAN has an appendix that addresses NetD requirements. However, in addition to providing for preventive network protection, future OPLANs should identify the systems critical to performing traditional warfare operations (e.g., logistics networks, command and control nodes, etc.). Moreover, we should pinpoint high-threat adversaries so we can begin planning and coordinating cyber engagement operations, and we should plan and execute targeting operations on mission-critical systems identified by the COCOM. However, this time if we discover the adversary, we should commence engagement operations to affect or influence him.

Two important points merit emphasis. First, the adversary discovered during targeting operations might be entirely different from the one addressed by the OPLAN—a possibility that makes cyberspace such a challenging domain to dominate. Second, targeting and engagement operations do not necessarily have to be linked to a specific COCOM OPLAN. We can perform proactive targeting operations as long as we properly delineate and synchronize them with other operations. We should consider performing engagement operations every time we discover a network intrusion, whether through traditional detection techniques or targeting operations.

Conclusion

According to the 67th Network Warfare Wing, "The bottom line is that the Air Force must transition from a detection-centric orientation to an active network kill chain approach which integrates prevention, detection, response, and adversary engagement."[13] This vision cannot come to fruition without organizing and tasking NetD operational units to change their operational constructs from a reactive approach (monitor, detect, and respond) to one that, as recently described by Lt Gen William T. Lord, "seek[s] out threats and . . . detect[s] and defeat[s] them instantaneously."[14] We cannot do this in isolation. We need purposeful planning and coordination with intelligence and national-level agencies. Furthermore, the creation of US Cyber Command should help ensure that services act under the authority and direction of a COCOM. The cyber targeting and cyber engagement constructs truly "operationalize" NetD since they focus squarely on acting upon and affecting the adversary. In the future, we should pay comparable attention to mission assurance (i.e., continuing operations despite enemy attacks), an area that prevents the complete separation of

NetD and NetOps. However, we cannot adequately address it without planning and very good intelligence. The DOD spends $100 million every six months to defend the .mil network.[15] At some point, we must ask ourselves whether we are reaching our defensive goals and deterring adversaries. Today, we are not, but by operationalizing NetD and concentrating on affecting the enemy, we can reverse this trend so that the Air Force can fight back. ✪

Lackland AFB, Texas

Notes

1. Air Force Program Action Directive 07-08, *Phase One of the Implementation of the Secretary of the Air Force Direction to Organize Air Force Cyberspace Forces*, 19 December 2008, 8.

2. Air Force Instruction 33-115, vol. 1, *Network Operations (NETOPS)*, 24 May 2006, 3, http://www.af.mil/shared/media/epubs/AFI33-115V1.pdf (accessed 13 May 2010); and Air Force Doctrine Document 2-5, *Information Operations*, 11 January 2005, 20, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_5.pdf (accessed 13 May 2010).

3. Joint Publication 3-13, *Information Operations*, 13 February 2006, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (accessed 13 May 2010).

4. Spyros Antonatos et al., "Defending against Hitlist Worms Using Network Address Space Randomization," *Computer Networks* 51, no. 12 (22 August 2007): 3471–3490; and Dorene Kewley et al., "Dynamic Approaches to Thwart Adversary Intelligence Gathering," in *Proceedings of the DARPA [Defense Advanced Research Projects Agency] Information Survivability Conference and Exposition*, vol. 1 (2001), 176.

5. "Engaging the Adversary on Air Force Networks," Information Assurance Technology Analysis Center Report, TAT 04-25, DO 232, 5 March 2007, 1.

6. Chairman, Joint Chiefs of Staff, to distribution list, memorandum, subject: National Military Strategy for Cyberspace Operations (without enclosure), December 2006, 13, http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed 14 May 2010).

7. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 87.

8. *Attribution* means the degree of confidence with which we can identify the adversary.

9. John P. Stenbit, assistant secretary of defense for command, control, communications, and intelligence, to secretaries of the military departments et al., memorandum, subject: Guidance for Computer Network Defense Response Actions, 26 February 2003, https://powhatan.iiie.disa.mil/cnd/cnd-ra-matrixand-memo.pdf (accessed 14 May 2010).

10. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 84.

11. Field Manual 3-01.7, *Air Defense Artillery Brigade Operations*, 31 October 2000, 6-36, http://www.theblackvault.com/documents/fm3_01x7.pdf (accessed 14 May 2010).

12. White House, *The National Strategy to Secure Cyberspace* (Washington, DC: White House, February 2003), http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (accessed 14 May 2010) .

13. 26th Network Operations Group, "NetD Concept of Employment," final draft, 14 December 2007, 2.

14. Chuck Paone, "General Calls for New Thinking on Cyberspace," 12 May 2009, http://www.af.mil/news/story.asp?id=123148876 (accessed 8 April 2010).

15. William Jackson and Doug Beizer, "New DOD Cyber Command Will Focus on the Dot-Mil Domain," *Government Computer News*, 15 June 2009, http://gcn.com/Articles/2009/06/15/Web-DOD-cyber-command.aspx?p=1 (accessed 8 April 2010).

Satellites and Remotely Piloted Aircraft

Two Remotely Operated Ships Passing in the Fight

Col Keith W. Balts, USAF*

Don't fire until you see the whites of their eyes!

—Col William Prescott
Battle of Bunker (Breed's) Hill, 1775

Combat identification for unmanned aircraft systems (UAS) during time-sensitive targeting can be messy and may include inputs from the distributed common ground/surface system, the combined air and space operations center, the ground commander, and, of course, the UAS pilot.

—Pilot of a remotely piloted aircraft
Operation Enduring Freedom

Advances in technology allow modern forces to fight battles at extreme distances, separating the shooter from the target. Whereas Colonel Prescott delivered his famous directive in person and on the battlefield, the ground commander in Afghanistan communicates with the remotely piloted aircraft (RPA) unit in Nevada while inputs stream in from the distributed common ground/surface system in Virginia and the combined air and space operations center in Qatar.[1] Like RPA operations, space operations are distinguished by vast geographic separation between the ground and (space) vehicle segments. According to Gen Kevin Chilton, commander of US Strategic Command, space operations are "absolutely global in nature and indifferent to physical terrain or lines drawn on a map."[2]

Forces able to distribute their operations geographically can gain advantages in force protection, economy of force, flexibility, and system and personnel costs; however, such distribution also exposes them to unique vulnerabilities and challenges. With the advantages in mind, the military has already fielded many remotely operated systems or has them under development, demonstrating an evolutionary trend toward more, not fewer, distributed operations. The RPA example above is a prolific one in the air domain; examples exist in other physical domains as well. General Chilton has punctuated the growing reliance on distributed operations for the space and cyberspace domains, identifying them both as media "in which the United States can expect to be challenged."[3] In general, fourth-generation warfare theory also supports this trend by suggesting that military operations are more "likely to be widely dispersed and largely undefined."[4]

In light of this relatively new trend, military leaders need to consider potential second-order effects, uniquely associated with distributed capabilities, that may detract from the advantages that these capabilities bring to the fight. Comparing space and RPA operations illuminates several of these effects. By leverag-

*The author is vice-commander of the 30th Space Wing, Vandenberg AFB, California.

ing the experience gained from decades of space operations, military leaders can translate applicable lessons learned from a relatively mature unmanned community to a comparatively young one. Many of these lessons also apply to remotely operated capabilities in other domains.

Why should we compare space and RPA operations? Of all the terrestrially based remotely operated systems, RPAs currently make up the preponderance of those systems distributed across significant distances—that is, outside the immediate area of responsibility. Operators of other remote systems are in fairly close proximity to the vehicles they control, but those systems may grow more distributed over time; thus, their communities could also benefit from this discussion. Unlike the recent trends in air, land, and sea domains, historically, space operations have always been distributed (and remotely operated) due to the unique physical attributes of, technical challenges peculiar to, and risks in the space domain. As Gen C. Robert Kehler, commander of Air Force Space Command (AFSPC), remarked during a visit last year to Creech AFB, Nevada, home of Air Force RPAs, "We understand remote split operations in AFSPC. We have been operating UASs for many years. It's just that those UASs fly outside the atmosphere, and we fly things that are more than 22,000 miles away. We do that with remote split operations."[5] Military space operations do involve several *manned* weapon systems, especially ground-based platforms performing space-related missions. Examples include launch vehicles, most space situational-awareness sensors, and space-control systems with a direct physical, rather than a remote, connection to the weapon system; however, this article addresses satellites because they represent the preponderance of space operations and are, in essence, remotely operated space vehicles. Satellite system architectures closely resemble RPA architectures since both consist of control segments, vehicle segments, and the links connecting them.

Nevertheless, the crisscrossing evolutions of satellites and RPAs distinguish the two. On the one hand, space operations began in a distributed mode but have grown closer to the fight by deploying new systems and expertise into the theater of operations.[6] RPA operations, on the other hand, distribute key elements of traditional air operations away from the theater. Despite their differences in capability and operating domain, space and RPA operations share enough characteristics to make them worthy of comparison as examples of distributed operations.

Background, Analysis, and Embedded Recommendations

With the space community's more than five decades of experience in distributed operations, what lessons apply to the RPA community? The doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) construct used by the Joint Capabilities Integration and Development System, offers a framework for comparison and analysis.[7] A DOTMLPF analysis of space operations reveals some recommendations that can help remotely operated communities in other domains better prepare for future distributed operations.

Doctrine

Despite the importance of doctrine to military success, especially the effective employment of new technologies, military personnel have noticed a lack of an overall doctrine for RPAs.[8] The uniqueness of these aircraft and other remotely operated systems warrants specific guidance to address shortfalls and differences in existing doctrine.

Current command and control (C2) doctrine posed significant challenges to space operations in the late 1990s and early 2000s as space capabilities became more integrated with traditional military operations.

Most of these hurdles concerned command relationships, more specifically, the best way to present space forces and command and control them during major military operations.

Two nuances, unique to space operations at the time, forced leaders in-theater and in US-based space organizations to reexamine existing C2 doctrine for establishing command relationships. First, space units can create effects within the traditional area of operations without the need to fully deploy or undergo a change of operational control (CHOP) to theater. Second, space capabilities can create effects across the entire area of operations—even across multiple areas of responsibility simultaneously or within the same tactical timeframe (i.e., a single execution cycle for satellite planning, similar to a single Global Hawk sortie).

Traditional criteria for establishing command relationships did not address these nuances, so conflict ensued between supported and supporting commanders over how best to resolve this doctrinal gap. After years of experimentation, exercises, operational experience, and heated exchanges, the Air Force developed specific doctrinal criteria to help commanders establish the appropriate command relationships, such as operational control, tactical control, or a supporting affiliation.[9] Using this doctrine as a baseline, the RPA community should establish exact criteria for defining command relationships when units do not need to fully deploy or when their weapon systems can create simultaneous effects across traditional areas of operations.

Organization

During the past two decades, space expertise and organizations evolved within geographic commands in order to better integrate space capabilities into traditional military operations; advise senior theater leadership on space capabilities; and plan, coordinate, and execute theater space operations. The speed and effectiveness of this evolution depended on the location and organizational affiliation of the space personnel involved.

Initially, very few space-savvy personnel existed outside of US Space Command (USSPACECOM) to assist theater commanders in integrating these new capabilities.[10] Similarly, theater expertise did not flow back into USSPACECOM to help career space officers understand the environment, requirements, and culture of traditional military operations. To remedy this situation, in the mid-1990s USSPACECOM, AFSPC, and their equivalents from other services began deploying space support teams to theater organizations for planning, exercises, and real-world operations. The next step involved creating a permanent presence in major theater headquarters using liaison officers—specifically, officers working side by side with theater leadership but reporting to USSPACECOM or its subordinates. Finally, the Air Force assigned space experts—mostly graduates from the space course at the US Air Force Weapons School—to major theater headquarters, reporting directly to theater commanders. This evolution from deployable teams to liaison officers to permanent-party experts was a key element in increasing the effectiveness of space capabilities as geographic theater commanders gained more influence over space requirements and integration.[11]

While this evolution occurred at the junior-officer level, a similar one occurred at the senior level, although it lagged the junior-level process by several years. Senior space officers served as liaison officers, deployed, and then eventually became permanent members of theater headquarters as directors of space forces (DIRSPACEFOR), positions created to facilitate coordination, integration, and staffing activities in support of space-integration efforts for the combined force air component commander.[12] A critical milestone, establishment of the DIRSPACEFOR position gave space operations a forum and voice in theater headquarters that junior officers could not always provide. It also enabled senior

space leaders to gain direct experience in theater operations.

RPA operations had their roots in theater operations, but the evolution of theater space organizations is noteworthy because it demonstrates a desired end state for expertise in distributed operations. If the RPA community succumbs to the temptation to distribute too much expertise away from the theater, it could find itself in the same situation as the space community in the early 1990s. By keeping sufficient junior- and senior-level RPA experts embedded within theater organizations, rather than relying on liaisons, the RPA community will ensure effective integration of current and future capabilities. Although not examined here, several organizational changes also occurred inside space organizations to better support theater activities.

Training

Distributed operations carry with them the disadvantage of simultaneous authorities exercised over a single unit by both the "organize, train, and equip" chain of command of their military service and the operational chain of their combatant commands. When units do not CHOP into or out of a theater, commanders experience a dilemma in unity of command in that they must fight a war while they train for it. Space operations mitigate this disadvantage by establishing recurring training requirements for line crews and real-world proficiency standards for training and evaluation personnel (as well as unit leadership). Having to perform periodic real-world operations not only keeps instructors and evaluators proficient, but also enables them to help backfill line crews so the crews can interrupt their normal schedule rotation to fulfill monthly training and evaluation obligations. Major system upgrades and procedural changes can also stress the steady-state manpower levels needed to balance training requirements and real-world operations. Manpower needs must account for potential surge capacity for major modifications to the weapon system, procedures, or real-world operations tempo. Policies and requirements put in place by the space community could serve as a baseline for RPA units that must also train while they fight.

Distributed operations offer a key training benefit insofar as recorded data can contribute to better debriefings of individual missions and help train other operators. Unfortunately, the exclusive use of this data can also lead operators to "drink their own bathwater" by learning the wrong lessons in the absence of external perspectives from supporting or supported forces. Collaboration tools and opportunities to visit related locations in person can generate these external perspectives. Funding for site visits, key conferences, and select debriefings will help distributed operators improve their performance; in turn, those operators will educate forward units on the capabilities and limitations of emerging weapon systems. In fact the first real benefits from the evolution of theater space organizations came from educating theater commanders on space capabilities, which also led to increased credibility for the space community.

Materiel and Facilities

Since satellites and RPAs differ widely due to the operational domains involved, materiel considerations worthy of comparison reside mainly in facilities associated with the control segment and communication links. Despite tight cost constraints, requirements for control nodes should include capacity for growth in both size and coordination demands. The ability to surge efficiently beyond routine mission objectives will enable operators to carry out infrequent but complex operations that necessitate crew augmentation, accommodate outreach opportunities without interfering with operations (i.e., hosting tours for external organizations), and integrate unforeseen future capabilities. Expanding part of the system without major redesign represents

another advantage of distributed systems over traditional manned systems.

The role of simulators in distributed operations also enters into a discussion of the materiel element. Control nodes for remotely operated systems depend heavily on computers and data manipulation, making their functionality easier to simulate than manned systems that operate in the physical environment. Simulators for distributed operations can be incredibly realistic, especially for weapon system displays that use text and graphics versus live video or audio feeds. Close synchronization of upgrades between real-world systems and simulators is paramount since both training and operations occur simultaneously.

Finally, effective distributed operations depend upon links to the outside world. These links are important not only for vehicle connectivity and situational awareness but also for operators to feel connected to the mission and the people they support or who support them. Similarly, realistic visualization tools and meaningful collaboration capabilities can amplify contributions made by personnel operating outside the traditional area of operations. Three-dimensional common operational pictures and training tools, along with live video feeds, assist operators in comprehending the environment not physically present around them. Video teleconferencing, live chat, and ample travel opportunities can also build and maintain professional relationships for successful collaboration, allowing operators to understand the nuances and nonverbal communication behind the inputs they receive. Protection of control nodes and links should also occupy a high position on commanders' lists of priorities since they often represent the most vulnerable aspects of the weapon system.

Leadership and Education

The crisscrossing evolutions of the space and RPA communities also produce useful comparisons for overcoming leadership and education challenges associated with distributed operations. Leaders of distributed operations face two significant obstacles—instilling a warrior ethos and motivating personnel who operate away from their "band of brothers" in the war zone. Some of this disconnectedness can even lead to post-traumatic stress disorder among RPA crews involved in lethal operations.[13] Even though space operations do not currently involve lethality, motivated operators with a warfighter mentality are still critical to mission success, especially personnel integrated directly with ongoing military operations. Initially, the RPA community has the benefit of drawing its personnel from manned systems—these individuals bring their deployed experience with them. The challenge lies in sustaining that perspective in their new community while educating the next generation of operators who might not have the benefit of theater experience. Video teleconferencing, instant messaging, and other electronic collaboration methods can go only so far in creating and sustaining a feeling of connectedness with other personnel and weapon systems involved in the operation beyond the immediate control node. The experience is just "not as potent an emotion as being on the battlefield."[14] Distributed operations may yield huge cost savings and reduce risk, but to periodically connect operators with the battlefield, commanders should allocate funding and manhours for trips to the theater and other distributed elements. Waiting three years for new operators to take on a liaison or embedded RPA position in-theater is too late to benefit the mission during their first operational tour.

Personnel

The military space community grew out of an engineering culture whose early space operators included either officers with technical degrees or technically savvy contractors. In the 1990s, the Air Force transitioned to nontechnical officers and eventually to enlisted personnel as the mainstay of space operations, at the same time keeping con-

tractors involved to balance the loss of technical expertise. Although this move helped operationalize space capabilities and save money, the pendulum had swung too far, diluting experience at the junior and midcareer levels. The Air Force reacted by pushing for more technical, advanced degrees and for specialization within the career field to counter the degradation in technical proficiency. Moreover, the conversion to enlisted personnel cost young officers early opportunities to gain this expertise as part of their professional development. It is difficult to develop senior leaders in a community that offers few opportunities to acquire technical experience at a junior level. (Approximately 75 percent of second-tour space officers served as missileers in their first assignment.)[15]

In summary, the RPA community should not abandon its origins even though technology permits it to do so. Rapidly training new officer accessions or enlisted personnel to operate RPAs may seem attractive, but such policy changes should occur gradually, allowing commanders to identify and resolve second- and third-order effects before drastic corrections become necessary.

Conclusion

Distributed operations offer unique advantages in warfare, but they can also include serious side effects. By examining space operations and applying lessons learned to other distributed operations, military leaders can minimize negative second-order effects and thereby ensure mission success.

Lessons within each DOTMLPF element can prevent the repetition of mistakes when new domains open or when remotely operated systems appear in the existing operational environment. Distributed operations stretch our current understanding of established domains, thus driving the need for unique doctrine and organizational structures. Furthermore, personnel policies, leadership development, and training programs must adapt to incorporate nuances never before encountered in traditional warfare—or at least not encountered to the extent revealed by modern distributed operations. Finally, placing more emphasis on the design of control nodes, perhaps at the expense of some vehicle prominence, will allow leaders to leverage the most versatile and flexible segment of distributed weapon systems.

By taking a hard look at how space operators approached these elements, military leaders can improve the integration, evolution, and mission contributions of newer distributed systems such as RPAs. As space operations evolve toward and RPAs evolve away from their traditional operating environments, they learn many lessons for sharing—like two remotely operated ships passing in the fight. ✪

Vandenberg AFB, California

Notes

1. National Park Service, "Bunker Hill Monument," http://www.nps.gov/bost/historyculture/bhm.htm (accessed 22 September 2009); and Joseph L. Campo, to the author, e-mail, 28 September 2009.

2. Gen Kevin P. Chilton, "Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities," *Air and Space Power Journal* 23, no. 3 (Fall 2009): 5, http://www.airpower.au.af.mil/airchronicles/apj/apj09/fal09/fal09.pdf (accessed 21 May 2010).

3. Ibid., 6.

4. William S. Lind et al., "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette* 85, no. 11 (November 2001): 66.

5. Military doctrine does not specifically define *remote split operations*; rather, the term refers to operations described in this paragraph in which the operator and platform are geographically separated from each other. SSgt Alice Moore, "AFSPC Com-

mander Visits UAS Operations at Creech AFB," Schriever Air Force Base, 25 March 2009, http://www.schriever.af.mil/news/story.asp?id=123141399 (accessed 21 May 2010).

6. Maj Keith W. Balts, "The Next Evolution for Theater Space Organizations: Specializing for Space Control," in *Space Power Integration: Perspectives from Space Weapons Officers*, ed. Lt Col Kendall K. Brown (Maxwell AFB, AL: Air University Press, December 2006), 124, http://www.au.af.mil/au/aul/aupress/Books/Brown/brown.pdf (accessed 21 May 2010).

7. Sean C. Sullivan, "Capabilities-Based Planning: Joint Capabilities Integration and Development System and the Functional Capabilities Board," course reading (Newport, RI: Naval War College, 20 August 2008), 4.

8. P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-first Century* (New York: Penguin Press, 2009), 210.

9. Air Force Doctrine Document (AFDD) 2-2, *Space Operations*, 27 November 2006, 10–14, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_2.pdf (accessed 21 May 2010).

10. Today, USSPACECOM's space-operations mission resides in US Strategic Command.

11. Balts, "Next Evolution," 124.

12. AFDD 2-2, *Space Operations*, 7.

13. Scott Lindlaw, "UAV Operators Suffer War Stress," *Air Force Times*, 8 August 2008, 1, http://www.airforcetimes.com/news/2008/08/ap_remote_stress_080708/ (accessed 9 January 2010).

14. Singer, *Wired for War* (see caption for third unnumbered plate in the photo gallery following p. 308).

15. US Air Force, "13S Career Paths, Deliberate Force Development," briefing, AF/A3O-ST, January 2009, slide 21.