ASPJ
AIR & SPACE POWER JOURNAL

NOVEMBER–DECEMBER 2013
VOLUME 27, NO. 6
AFRP 10-1

Features

Departments

Editorial Advisory Board

Board of Reviewers

Search and Rescue in the High North

An Air Force Mission?

Col John L. Conway III, USAF, Retired

> *There are strange things done in the midnight sun*
>
> *By the men who moil for gold.*
>
> —Robert W. Service

The "Bard of the Yukon" would be surprised at the strange new things in the land of the midnight sun. What wouldn't surprise him are the things that never change: six months of darkness, constant danger, numbing cold, and adventurers planning to brave all three in search of fame, fortune, or just "a good look around." Some of their motivations include untapped oil and natural gas deposits, unprecedented (to known history) melting of Arctic ice, a quest for territorial rights, the lure of the fabled Northwest Passage, and "adventure tourism." All have resulted in greatly increased human activity—and with that comes the increased risk of human calamity by the unwise, the unprepared, or the unlucky. Capt Melissa Bert, former captain of the port and commander of Coast Guard Sector Juneau, echoes these concerns: "I don't worry about a war in the Arctic. . . . But I do worry that we're not prepared to deal with a major disaster there. No one is, but as more people go there, it becomes much more likely."[1]

A Question of Untapped Resources

The 2008 US Geological Survey estimate of High North energy resources, considered the most authoritative survey to date, suggests that 13 percent of the world's undiscovered oil and 30 percent of its undiscovered natural gas lie in the Arctic.[2] This amounts to approximately 90 billion barrels of oil; 1,669 trillion cubic feet of natural gas; and 44 billion barrels of liquid natural gas—a total exceeding all other known quantities of oil and natural gas in the Arctic.[3] Since most Arctic territory has been claimed, in practical terms the "race" for these exploitable natural resources is just about over. However, economic exploitation via leasing rights and transportation nodes remain as two powerful incentives.

Because many of these resources lie in relatively shallow (500 feet) coastal waters, they are "technically recoverable" but not necessarily "economically recoverable"—that is, no current infrastructure exists to develop offshore oil and gas in the Arctic, particularly in North America. Estimates indicate that a decade or more may pass before both capital and technology are available to begin the extraction process in earnest.[4] Royal Dutch Shell's highly publicized and very expensive (more than $4.5 billion) attempt to be the first to drill extensively in the Chukchi Sea highlights these problems. In 2012 the company drilled only modest exploratory wells, far short of its planned six deep wells, before abandoning efforts as the end of the short season approached. Later, its drill ship ran aground on an uninhabited island 300 miles southwest of Anchorage, and calls for tighter environmental regulation of offshore exploration increased in the aftermath. Shell has cancelled plans for the coming exploration season, prompting others to take a long look at their proposed plans.[5] Nevertheless, the lure of this much untapped oil and gas cannot be forestalled for long, despite nagging concerns that similar disasters will occur in the early phases of exploitation and extraction.

The Passages across the Top of the World

The High North also holds the promise of a shorter transit between the Far East and Europe: the centuries-old dream of the Northwest Passage (fig. 1) and the opening of a maritime route across northern Russia. The Northern Sea Route, which closely follows the coastline along Russia's northern tier, has seen far more success in Arctic transshipment than its Canadian counterpart. Forty-six vessels transited this route in 2012, carrying over a million tons of cargo—a 53 percent increase in tonnage from 2011. More ships, aided by Russia's sizable (more than 30) fleet of icebreakers, will probably add to that total in the coming years, and China has announced its first commercial voyage there this summer.[6] Local maritime traffic supporting drilling operations continues to grow as well. Receding sea-ice coverage in the High North during the summer has made the long-sought-after Northwest Passage an emerging reality—at least in the late summer and early fall. Claims that the route would "rival the Suez Canal" and would be "ice free" by 2015 have grudgingly yielded to more measured assessments of both; yet, the promise of ice-free passage and a shorter sea route to and from Europe and Asia continues to gain traction and international attention.[7]

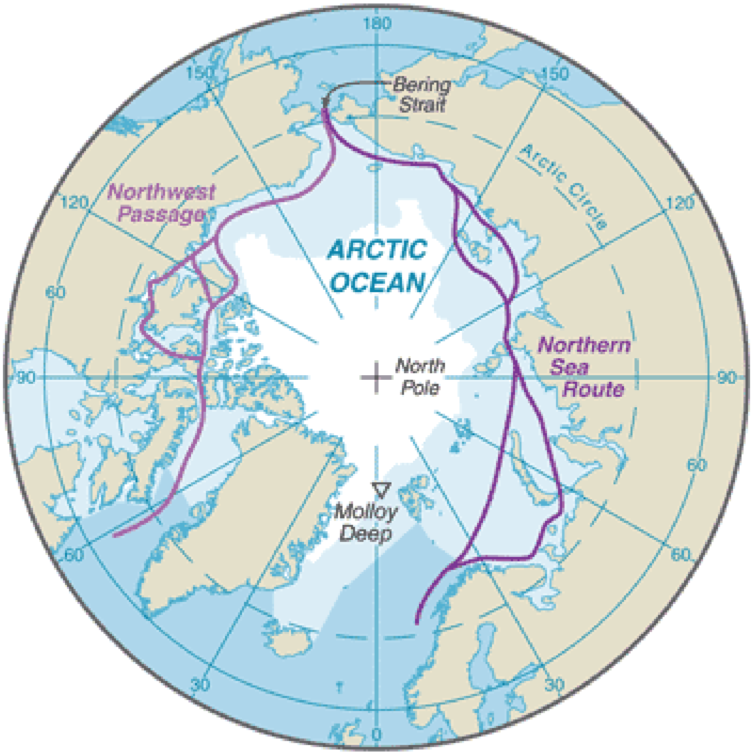


Figure 1. The Northwest Passage(s) and the Northern Sea Route. (Reprinted from "Arctic Ocean," in Central Intelligence Agency, *The World Factbook*, accessed 3 September 2013, https://www.cia.gov/library/publications/the-world-factbook/geos/xq.html.)

The Northwest Passage actually includes more than one route across the Canadian Archipelago, an expanse of territory consisting of 73 major islands and 18,114 smaller ones encompassing an area roughly the size of Greenland. The more southerly passage has a draft of only 13 meters while the one to the north has an average depth of 200 meters. The more southerly channel, the Union Strait, holds the promise of less ice but may be unavailable to deep-draft vessels. To the north, the recently opened (2007) McClure Strait is deeper but more ice laden.[8] A Norwegian study of 2011 lists no fewer than seven different routes through the Northwest Passage, explaining that the current navigation channel offers the best sea-ice conditions at the time.[9]

Although some observers use the term *ice free* to describe the Northwest Passage, one should do so with caution because even "open water" can contain icebergs. *Ice free* is a catchphrase for newspaper pundits, but experts prefer the more precise term *ice diminished*.[10] Furthermore, even that descriptor means that ice is still present. Canadian geographer Frédéric Lasserre points to multiseason ice formations (frozen, thawed, and refrozen) that are particularly dense and very difficult to spot as a significant hazard to navigation throughout any "ice free" or "ice-diminished" season.[11]

University of British Columbia professor Michael Byers agrees, adding that thinning ice produces more icebergs in Eastern Arctic waters as Greenland's glaciers move more quickly into the sea. Glacial ice is very hard, he explains, and glacier ice "growlers" are particularly dangerous even to "ice-strengthened" ships—those with reinforced hulls but no ice-breaking capability. Nevertheless, the sinking of the ice-strengthened passenger ship *MS Explorer* in the Antarctic in 2007 stands as a stark example of what can happen when even such a vessel meets multiyear ice.[12] The Norwegian assessment paints an even bleaker picture. Refuting the term *ice free*, it contends that "most Arctic shipping experts view this term as meaning ice-infested with icebergs, bergybits and growlers present," concluding that "from a mariners [*sic*] point of view ' . . . with less ice, more icebreaking capacity will be needed.'"[13]

Perhaps the most measured discussion—out of dozens of contrary claims—of impending Arctic ice melt comes from the Center for Climate and Energy Solutions in its paper *Climate Change & International Security: The Arctic as a Bellwether* (2012).[14] That study lists three dates for an ice-free (i.e., 80 percent loss of historical sea ice during the summer) Arctic based on linear and nonlinear extrapolations of minimum sea-ice extent in the summer. Not surprisingly, these projections vary widely from 2025 to 2072.[15] Insurer Lloyds of London, more interested in the bottom line than in bombast, agrees with the midrange scientific forecasts but warns that thinner ice may mean more wave action and more abrupt destruction of the ice pack, thus adding to the overall uncertainty. In reality the Northwest Passage is a complex dynamic of ice, islands, and changing weather conditions that make transit a challenge and disaster only one poor decision away.

Enthusiasts extol the shorter shipping routes through the Arctic and forecast a renaissance in polar shipping, but this is not the case. Shipping to Asia from Mediterranean ports (Marseilles to Shanghai, for example) provides no distance-based economic advantage while high-latitude to high-latitude destinations—say, Marseilles to Yokohama—do offer such an advantage. An analysis of 20 city-pairs that might use the Northwest Passage or the Northern Sea Route found that only three are shortest through the Northwest Passage.[16] Regardless, the lure of shorter maritime routes to and from the markets of Asia and Europe via the High North continues to draw more attention and increased human activity.

Today, only cruise liners, private adventurers, and a few commercial vessels journey through the Northwest Passage, but a significant uptick in transits (69 [1906–2006]; 40 [2010–11]; and upwards of 30 in 2012) worries search and rescue (SAR) experts who see potential disaster in an unforgiving environment.[17] Experts also point to poor navigational aids as a major contributor to safety concerns along the Northwest Passage. A *Wall Street Journal* article highlights the overarching issue of sea-bed mapping: “Overall, maps of Mars are about 250 times better than maps of the earth’s ocean floor.” Another report warns that at its current rate, completely charting Canadian Arctic waters will take three centuries.[18]

The Arctic Council and the Nuuk Search and Rescue Agreement

In 1996 eight nations with territory or clearly defined interests in the region (the United States, Canada, Russia, Finland, Norway, Denmark, Iceland, and Sweden) formed the Arctic Council “to provide a means for promoting cooperation, coordination and interaction among the Arctic States, with the involvement of the Arctic Indigenous communities and other Arctic inhabitants on common Arctic issues."[19] The council is unique in that it addresses only nonsecurity issues faced by the Arctic states; the region's indigenous peoples and observers characterize it as "populated more by scientists and scholars than by statesmen."[20] Mindful of its previous call in 2008 to "further strengthen search and rescue capabilities and capacity around the Arctic Ocean," the council signed a SAR treaty at Nuuk, Greenland, in 2011—the *Agreement on Cooperation on Aeronautical and Maritime Search and Rescue in the Arctic* (the *Nuuk Agreement*), which states that each party will establish and maintain an "adequate and effective search and rescue capability" within its designated area (fig. 2).[21] Further, it binds member nations to coordinate SAR efforts in case of a plane crash, cruise ship sinking, oil spill, or other disaster across the High North.[22]

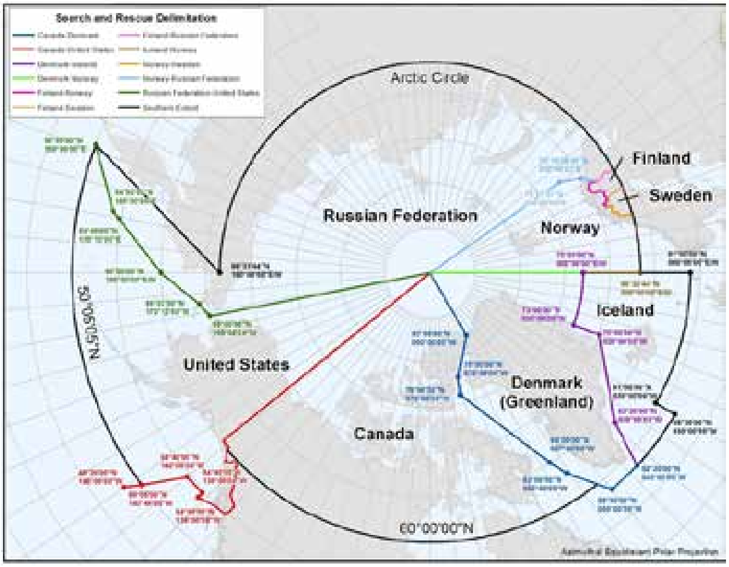
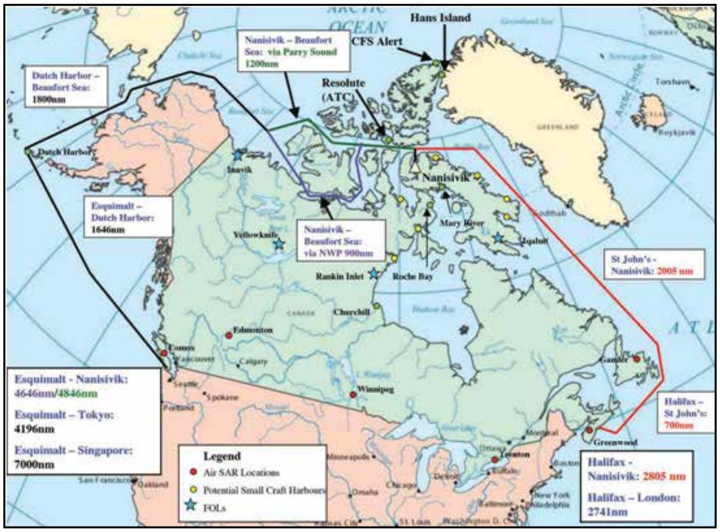


Figure 2. Arctic SAR agreement, areas of application. (Based on geographic coordinates in the annex to the *Agreement on Cooperation on Aeronautical and Maritime Search and Rescue in the Arctic*, 12 May 2011, http://www.ifrc.org/docs/idrl/N813EN.pdf. Map from "Arctic Search and Rescue Agreement," Arctic Portal, accessed 3 September 2013, http://arcticportal.org/features/751-arctic-search-and-rescue-agreement.)

The United States is responsible for SAR operations in Alaska and a large swath of the approaches to the Bering Strait. This also encompasses the western approaches to the Northwest Passage and the eastern approaches to the Northern Sea Route, paralleling Russia's Kamchatka Peninsula. The United States also has responsibility for SAR in the Beaufort, Chukchi, and Arctic Seas extending to the North Pole. Although not the largest area mentioned in the *Nuuk Agreement*, its size will tax US resources. A key point in the agreement—one that gives SAR planners pause—is that any party may request the assistance of any other party/parties if necessary, ensuring that "assistance be provided to any person in distress."[23]

In spite of increased successful transits of the Northwest Passage, news of three more passenger cruises in 2013 has raised concerns that a major disaster there would be met by a slow response from rescue forces—judged by some as too far away and too few in number to help quickly (fig. 3).[24] Placement of Canada's SAR assets highlights this potential dilemma: that country's lone rescue coordination center (RCC) at Trenton, Ontario, encompasses most of the Canadian Arctic, but it is located closer to the northern coast of South America, for example, than to the Canadian Forces Station in Alert, Nunavut.[25]


Arctic Ocean
Hans Island
Nanisivik – Beaufort Sea: via Parry Sound 1200nm
CFS Alert
Dutch Harbor – Beaufort Sea: 1800nm
Resolute (ATC)
Dutch Harbor
Inuvik
Nanisivik
Mary River
Iqaluit
Esquimalt – Dutch Harbor: 1646nm
Yellowknife
Nanisivik – Beaufort Sea: via NWP 900nm
St John's - Nanisivik: 2005 nm
Rankin Inlet
Roche Bay
Churchill
Edmonton
Comox
Vancouver
Calgary
Esquimalt - Nanisivik: 4646nm/4846nm
Esquimalt – Tokyo: 4196nm
Esquimalt – Singapore: 7000nm
Winnipeg
Gander
Halifax – St John's: 700nm
Greenwood
Trenton
Legend
● Air SAR Locations
○ Potential Small Craft Harbours
☆ FOLs
Halifax - Nanisivik: 2805 nm
Halifax – London: 2741nm
Greenland
Reykjavik
Torshavn

FOLs - forward operating locations
nm - nautical miles
NWP - Northwest Passage

Figure 3. Operational Arctic patrol distances. (Reprinted from Michael Byers and Stewart Webb, *Titanic Blunder: Arctic/Offshore Patrol Ships on Course for Disaster* [Ottawa: Rideau Institute, Canadian Centre for Policy Alternatives, April 2013], 37, http://www.policyalternatives.ca/sites/default/files/uploads/publications/National%20Office/2013/04/Titanic_Blunder.pdf.)

Flight time from Winnipeg to Resolute Bay in the heart of the Northwest Passage via a Canadian C-130H is over five hours; helicopters to the same area from Comox would take more than 11.[26] Although a Canadian Forces CC-177 (the Canadian version of the USAF C-17) demonstrated that it can land and take off from Canadian Forces Station Alert's 5,500-feet gravel runway, it is not Canada's primary SAR aircraft and may not always be available for that mission.[27] Defenders of the current aircraft-basing concept point out that most rescues occur in southern Canada, not in the High North. However, pressure is growing to expand Canadian Arctic SAR presence northward. Canada's major High North maritime assets—its two icebreakers—confront the daunting task of patrolling the Northwest Passage's 1,200 nautical miles.[28] So far, luck has been on their side. In 2010 the 120 passengers on the ice-strengthened "elderly expedition cruise ship" *Clipper Adventurer* were evacuated by a nearby (two days' sailing) Canadian Coast Guard icebreaker after the cruise ship ran aground in the Beaufort Sea's Coronation Gulf.[29] Air and sea traffic is growing rapidly in the High North, increasing the likelihood that mishaps will occur. Given the paucity of Canadian assets—both in quantity and placement—chances that the United States may be asked to assist Canadian rescuers are also growing.

The US Role in High North SAR: It's the Coast Guard's Job

According to the *Nuuk Agreement*, the Coast Guard is the US "competent authority" for SAR efforts. More importantly, it lists both that service and the Department of Defense as the US SAR "agencies." US RCCs in the agreement include the Aviation Rescue Coordination Center–Elmendorf at Joint Base Elmendorf–Richardson (JBER) and the Joint Rescue Coordination Center–Juneau, Alaska.[30] Although the Coast Guard has permanent bases in Alaska, all are located below the Arctic Circle. Coast Guard aircraft are permanently based in Kodiak, about 800 miles south of Point Barrow, requiring transit of the 9,000-feet-high Brooks Range to the North Slope. The nearest major port to Point Barrow is in the Aleutian Islands, another 500 miles south, and this spring the Coast Guard announced that it had no plans to build any shoreside infrastructure in the coming decade.[31] Draconian cuts to the service's fiscal year 2014 budget request fell heaviest on its aviation assets, limiting its near-term aviation-response options.[32]

The *United States Coast Guard High Latitude Region Mission Analysis Capstone Summary* study of 2010 also called for a significantly larger icebreaker fleet to augment the Coast Guard's one medium and one heavy icebreaker, but the fiscal year 2014 budget request includes only $2 million for design studies for an approximately $1 billion 10-year project.[33] Building only one won't be enough: three heavy and three medium icebreakers are needed just to meet the Coast Guard's minimum statutory requirements.[34] The service's 2013 *Arctic Strategy* lists "broadening partnerships" as one of its strategic objectives but does not specifically detail who these partners will be.[35]

The year 2014 may prove pivotal in the High North for the Navy's Arctic plans. Its 2009 *Arctic Roadmap* defers any major Arctic force-structure decisions until the 2014 *Quadrennial Defense Review Report*. Even if the Navy proposes an increased Arctic role in that report, funds and equipment will not be available for a decade or more.[36] A common thread in the Navy's *Roadmap*, the Coast Guard's *High Latitude Region Summary*, and its new *Arctic Strategy* is the absence of any disaster-response alternatives beyond icebreakers and organic Coast Guard / Navy aviation assets—to the conspicuous exclusion of the Air Force. The latter is briefly mentioned in the Navy's *Roadmap* regarding "existing agreements" as well as "satellite surveillance and weather operations" but is invisible in the Coast Guard's *High Latitude Region Summary* and its *Arctic Strategy*.[37]

Nevertheless, there remains an overarching requirement that the United States assist signatories of the *Nuuk Agreement* if called upon. Russia, with its 30-plus icebreakers, significant Arctic population, and reawakened Northern Fleet, seems capable of conducting SAR without outside help. Canada, however, may need our assistance in the Northwest Passage to augment its limited resources. Both Canada and Greenland may request US help for SAR on the eastern approaches to the Northwest Passage.

"Who Ya Gonna Call?"

Air Force assets already perform SAR missions in Alaska, coordinated through the 11th RCC at JBER, using helicopters and fixed-wing aircraft of the Alaska Air National Guard's 176th Wing.[38] All Air Force aircraft in Alaska should be part of any SAR effort, particularly along the Northwest Passage, the approaches to the Bering Strait, and into the Beaufort and Chukchi Seas. Moreover, the Air Force has the resources and ability to reach any High North disaster faster than other surface vessels—US, Canadian, or otherwise—and to provide command, control, and communications support until the crisis is resolved. Its approach to SAR in the High North should center on three elements: bases, aircraft, and partnerships.

Bases

Two Air Force bases sit well above 60 degrees, well positioned for launch and recovery of any SAR effort: Eielson AFB at 64°39’56” N and Thule Air Base (with its 10,000-feet runway), 750 miles north of the Arctic Circle at 74°31’52” N. South of Eielson is JBER with another 10,000-feet runway as well as the 11th RCC. At the outer edge of the Aleutian Island chain sits Eareckson Air Force Station (formerly Shemya AFB), a contractor-maintained alternate / emergency landing field / refueling location and the site of an Air Force “Cobra Dane” radar installation. Eareckson’s 10,000-feet runway and several hangars constitute a far-western basing resource for any SAR operation.

Aircraft

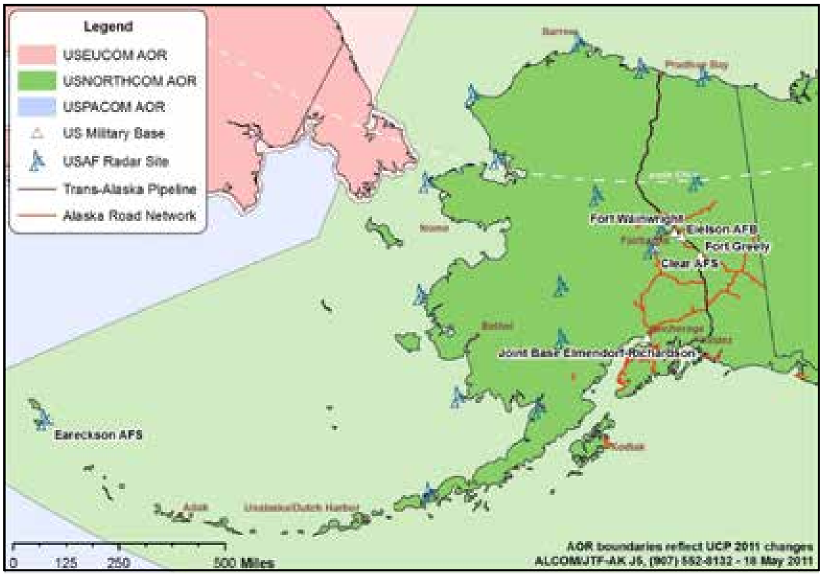
The number and variety of Air Force aircraft available at Eielson and JBER would greatly expand SAR response options. Eielson is home to the 354th Fighter Wing (F-16s) and the Alaska Air National Guard’s 168th Air Refueling Wing. JBER hosts the Air National Guard’s 176th Wing (C-17s and C-130s as well as HC-130 and HH-60G SAR aircraft). It also hosts the Air Force’s 3rd Wing, with C-17s, C-12s, the E-3 Airborne Warning and Control System aircraft, a number of fighters, and two air and space operations centers. Since Canada has shown that C-17s can operate from a 5,500-feet gravel runway in northern Canada, Air Force C-17s could do the same.[39]

Another SAR asset (outside Alaska), the New York National Guard’s ski-equipped 109th Airlift Wing, has extensive experience in the Antarctic and has performed missions for the National Science Foundation in the Arctic. Aircraft rotations to Alaska, much like their Antarctic temporary duties, could augment other assets and bring another option for SAR. Remotely piloted aircraft can play a role as well. The *Navy Arctic Roadmap* called for those platforms to do “data collection, monitoring and research," but SAR missions using Global Hawks could add a persistent overwatch asset for the entire region.[40] Global Hawks could cover an area up to the North Pole and—winds and weather permitting—across the entire length of the Northwest Passage and its approaches.[41]

We must emphasize that High North SAR is not a year-round mission despite imminent "ice-free" claims. The peak season for activity—March to early October—will remain predictable for some time to come. In keeping with the Office of the Secretary of Defense's policy that "SAR . . . is not a force sizing or shaping mission for [the Department of Defense]" but that the department will contribute "when needed and as available," no new SAR assets would be created.[42]

Partnerships

Coordination of the Air Force's SAR efforts may constitute the greatest challenge. For example, the 2011 *Unified Command Plan* realigned areas of responsibility (AOR) in the High North (fig. 4). Previously, US Pacific Command (PACOM) had an area from the Bering Strait to the North Pole and west along the Siberian coast to the Kara Sea. The 2011 realignment kept the Russian Pacific littoral in PACOM's AOR but nothing further north. Meanwhile, the eastern approaches to the Bering Strait, once a shared responsibility with US Northern Command (NORTHCOM), are NORTHCOM's alone. PACOM retains responsibility for the extreme western approaches to the Bering Strait and the seas adjacent to Siberian Russia but nothing further north or west. Responsibility for Alaska is now solely NORTHCOM's.



AOR - area of responsibility
USEUCOM - US European Command
USNORTHCOM - US Northern Command
USPACOM - US Pacific Command

Figure 4. US combatant command areas of responsibility in the High North. (Reprinted from Department of Defense, *Report to Congress on Arctic Operations and the Northwest Passage*, OUSD [Policy] [Washington, DC: Department of Defense, May 2011], 21.)

However, Air Force assets in Alaska are primarily owned by Pacific Air Forces (PACAF) (PACOM). This dichotomy means that NORTHCOM / Joint Task Force–Alaska must use Alaska-based PACAF (PACOM) aircraft to deter aggression, defend airspace, respond to natural and man-made disasters in the region, and conduct SAR. Simultaneously, PACAF must prepare these same Alaska-based resources to carry out PACOM's peacetime taskings and wartime training.[43] The eastern approaches to the Northwest Passage adjacent to Greenland and Canada's east coast are in US European Command's AOR, and NORTHCOM would have to coordinate with that command if any SAR request from that heavily traveled region came to the Department of Defense.[44] Further, the Air Force must form a strong partnership with the Coast Guard so that each can understand the other's mission and capabilities for conducting SAR. This synergy should benefit both organizations. Similarly, Canadian Forces and the Air Force must forge a working relationship for High North SAR, perhaps via North American Aerospace Defense Command. Finally, the Air Force should engage in a dialogue on Arctic issues with the newly formed Arctic Regional Studies Group at the Naval War College.

The Air Force must be prepared to assist in all High North SAR efforts in keeping with the *Nuuk Agreement*. However, this is no way implies that airpower can free an icebound ship or break pack ice ahead of an oil tanker headed to Nome. But the Air Force's resources (personnel, facilities, and aircraft) are available in an emergency—and because they *are* available, they should not be ignored.

The Future of the High North

The High North will see an increasing amount of international interest, activity, and investment in the coming decades. It possesses natural resources in abundance, but extracting them from an inhospitable environment will come at great cost. A navigable Northwest Passage is an accomplished fact, but it is a harrowing journey for the unwary and the unprepared. Its economic usefulness as a shortcut between Asia and Europe will grow over time, but those who travel it today may need assistance if not outright rescue. Increased traffic in the Bering Strait will challenge the abilities of Russian and US authorities to maintain safe passage.

The Arctic Council has proven that it can manage the region through consent of its members, yet other nations outside the region will test its self-imposed limits of authority for the benefit of their own agendas. The United States will become chairman of the Arctic Council when Canada's term expires in 2015 and will face more human activity in the region than in all previous decades combined. At the same time, the probability that some of the ventures listed above will come to grief will rise each summer season.

Current/projected North American SAR forces are inadequate to the task because of distance and available resources. Using all of the latter to effect a rescue is not only wise but also imperative. Consequently, both the US Coast Guard and the Department of Defense may be called upon to help our neighbor. Framing all of this is the *Nuuk Agreement*, which requires signatory nations to extend SAR help to any nation that requests it. The current silence by Coast Guard and Navy planners, as well as their reliance on surface rescues using scarce resources, is not consistent with the realities of time and distance. The Air Force is postured to help, but mounting a SAR effort without prior planning and coordination is not wise. It's time to add the weight of the Air Force to the effort, begin the coordination process, and prepare to assist. ✪

Notes

1. Peter Apps, "Melting Arctic May Redraw Global Geopolitical Map," Reuters, 3 April 2013, http://www.reuters.com/article/2012/04/03/us-arctic-resources-idUSBRE8320DR20120403. Captain Bert is currently chief of the Maritime and International Law Division at Headquarters US Coast Guard, Washington, DC.

2. US Geological Survey appraisal as quoted in standard briefing, Directorate-General for External Policies of the Union, Directorate B, Policy Department, European Parliament, subject: The Geopolitics of Arctic Natural Resources, 31 August 2010, 4, http://www.tepsa.eu/download/Valur%20Ingimundarson.pdf. See also US Geological Survey, "GIS Data: Circum-Arctic Resource Appraisal (North of the Arctic Circle) Assessment Units," 2009, http://energy.usgs.gov/RegionalStudies/Arctic.aspx#3886226-gis-data.

3. Seven areas in the Arctic contain about 87 percent of the known gas and oil reserves. Two are astride Greenland, three more hug the northern Russian coast and its adjacent waters, and the last two lie along the coast of Alaska and Canada's Yukon Territory. Most of the undeveloped natural gas lies in Asian Russia while the Arctic Alaska Basin is estimated to hold over 40 percent (29.96 billion barrels) of the entire total of undiscovered Arctic oil—more than three times as much as the next-largest field (the Amerasia Basin). All of this supposed bounty should be tempered by cold reality: oil and gas experts report that even if fully exploited, the Arctic fields will not replace the resources and capacity of the Middle East. Hobart King, "Oil and Natural Gas Resources of the Arctic," Geology.com, accessed 12 August 2013, http://geology.com/articles/arctic-oil-and-gas/.

4. Yue Wang, "Experts: Arctic Drilling for Security," UPI, 16 July 2012, http://www.energy-daily.com/reports/Experts_arctic_drilling_for_security_999.html.

5. Tom Fowler, "For Shell, Wait 'til Next Year in the Arctic," *Wall Street Journal*, 31 October 2012, B10, http://online.wsj.com/article/SB10001424052970204789304578086770366680196.html. The oil company Statoil of Norway announced it would delay its operations for at least a year while French oil giant Total said that environmental risks were too high to continue exploration in the Arctic. See also Tom Fowler and Ben Lefebvre, "Shell Puts Off Drilling in Alaska's Arctic," *Wall Street Journal*, 27 February 2013, B7, http://online.wsj.com/article/SB10001424127887324662404578330423854552576.html.

6. Trude Pettersen, "China Starts Commercial Use of Northern Sea Route," *Barents Observer*, 14 March 2013, http://barentsobserver.com/en/arctic/2013/03/china-starts-commercial-use-northern-sea-route-14-03.

7. Some selected headlines reinforce this notion of early ice melting: "Northwest Passage Channel Appears Free of Ice," Fierce Homeland Security, 16 August 2012; "Study Predicts Arctic Shipping Quickly Becoming a Reality," *Calgary Globe and Mail*, 4 March 2013; "Open Seas: The Arctic Is the Mediterranean of the 21st Century," *ForeignPolicy.com*, 29 October 2012; and (as late as May 2013) "White House Warned on Imminent Arctic Death Spiral," *Guardian*, 2 May 2013.

8. Frédéric Lasserre, "High North Shipping: Myths and Realities," in *Security Prospects in the High North: Geostrategic Thaw or Freeze?*, NDC Forum Paper 7, ed. Sven G. Holtsmark and Brooke A. Smith-Windsor (Rome: NATO Defense College, May 2009), 195, http://www.google.com/url?sa=t&rct=j&q=high%20north%20shipping%3A%20myths%20and%20realities&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fmercury.ethz.ch%2Fserviceengine%2FFiles%2FISN%2F102391%2Fipublicationdocument_singledocument%2F517b6a62-3f36-40be-a577-1f3a9337124c%2Fen%2Ffp_07.pdf&ei=nZoDUvq1OcugyQGuqoCIAw&usg=AFQjCNGyNDWmyKCgLcYMfHVHUA5rk13aHw&bvm=bv.50500085,d.aWc. Canada claims that the entire Northwest Passage falls within Canadian territory and must follow Canadian guidelines for passage, including asking permission. The United States, among others in the international community, contends that the entire passage is in international waters. This is not a "Fifty-Four Forty or Fight" type of dispute between the United States and Canada, but it does—on occasion—strain diplomatic relations.

9. Karl Magnus Eger, *Marine Traffic in the Arctic: A Report Commissioned by the Norwegian Mapping Authority*, ARHC2-04C (Oslo: Analyse & Strategi AS, 15 August 2011), 7–8, http://www.iho.int/mtg_docs/rhc/ArHC/ArHC2/ARHC2-04C_Marine_Traffic_in_the_Arctic_2011.pdf.

10. Ronald O'Rourke, *Changes in the Arctic: Background and Issues for Congress*, CRS Report for Congress R41153 (Washington, DC: Congressional Research Service, 24 July 2013), 58, http://www.fas.org/sgp/crs/misc/R41153.pdf. The report's 2012 data showed more polar ice melting at a faster rate, intensifying scientific discussion (ibid., 12).

11. Lasserre, "High North Shipping," 194.

12. Michael Byers, "Canada's Not Ready to Have the World in the Arctic," *Globe and Mail*, 15 August 2012, http://www.theglobeandmail.com/commentary/canadas-not-ready-to-have-the-world-in-the-arctic/article4481519/.

13. Eger, *Marine Traffic in the Arctic*, 8.

14. Rob Huebert et al., *Climate Change & International Security: The Arctic as a Bellwether* (Arlington, VA: Center for Climate and Energy Solutions, May 2012), http://www.c2es.org/publications/climate-change-international-arctic-security/.

15. Ibid., 11–12. Another interesting fact is that physics-based climate models show that the rate of ice loss will likely slow before the Arctic progresses to an ice-free state, which could cause an overestimation of the rate of future ice loss.

16. Lasserre, "High North Shipping," 192–95. Three others are roughly equidistant through either it or the Northern Sea Route.

17. Of all the transits of the Northwest Passage in 2012, only two were made by commercial vessels—the ice-strengthened tanker *Gotland Carolina* and the ice-strengthened passenger ship *Hanseatic*. "Alluring Northwest Passage—the Transit Tally So Far," Sail-World.com, 25 February 2013, http://www.sail-world.com/CruisingAus/index.cfm?SEID=2&Nid=106937&SRCID=0&ntid=0&tickeruid=0&tickerCID=0. Although this site indicated 24 transits, Canadian Coast Guard officials tallied 30 crossings of the Northwest Passage in 2012.

18. "U.S. Draws Map of Rich Arctic Floor ahead of Big Melt," *Wall Street Journal*, 31 August 2007, http://online.wsj.com/article/SB118848493718613526.html#articleTabs%3Darticle. An article of 2012 points out that only about 10 percent of Canadian Arctic waters are charted "to a modern standard." See K. Joseph Spears and Michael K. P. Dorey, "Arctic Cruise Ships: The Pressing Need for Search and Rescue," *Canadian Sailings*, 17 October 2012, http://www.canadiansailings.ca/?p=4830$print=1. See also Byers, "Canada's Not Ready."

19. "About the Arctic Council," Arctic Council, 7 April 2011, http://www.arctic-council.org/index.php/en/about-us/arctic-council/about-arctic-council. Denmark also represents Greenland and the Faroe Islands on the council.

20. Crocker Snow Jr., "Analysis: The Arctic Council, Lead Sled Dog of the High North," *GlobalPost*, 4 October 2012, http://www.globalpost.com/dispatch/news/regions/americas/121003/analysis-the-arctic-council-lead-sled-dog-the-high-north.

21. *The Ilulissat Declaration*, Arctic Ocean Conference, Ilulissat, Greenland, 27–29 May 2008, 2, http://www.oceanlaw.org/downloads/arctic/Ilulissat_Declaration.pdf; and the *Agreement on Cooperation on Aeronautical and Maritime Search and Rescue in the Arctic* [*Nuuk Agreement*], 12 May 2011, preamble and art. 3, par. 3, http://www.ifrc.org/docs/idrl/N813EN.pdf. In drawing the boundaries of those areas, the *Declaration* was careful not to assert that those boundaries won't be used as precedents for an unresolved boundary disputes (art. 3, par. 2).

22. Arctic Council, *Nuuk Declaration on the Occasion of the Seventh Ministerial Meeting of the Arctic Council, 12 May 2011, Nuuk, Greenland*, http://www.arctic-council.org/index.php/en/document-archive/category/5-declarations. Note that the 2011 *Nuuk Declaration* announced the 2011 *Nuuk Agreement* on SAR, among other things. This is the Arctic Council's first international treaty.

23. Ibid., art. 7, pars. 3 (d) and (e). The *Nuuk Agreement* also details each nation's "Competent Authority" (appendix 1), SAR agencies (appendix 2), and rescue coordination center (RCC) locations (appendix 3).

24. This includes transit of the world's largest private yacht (a floating condominium aptly named the *World*) in 2012. For a scathing attack on current Canadian plans for Arctic/offshore patrol boats, see Michael Byers and Stewart Webb, *Titanic Blunder: Arctic/Offshore Patrol Ships on Course for Disaster* (Ottawa: Rideau Institute, Canadian Centre for Policy Alternatives, April 2013), http://www.policyalternatives.ca/sites/default/files/uploads/publications/National%20Office/2013/04/Titanic_Blunder.pdf.

25. "The Arctic Is a Long Way from Canada's Search and Rescue Techs," Nunatsiaq Online, 3 November 2010, http://www.nunatsiaqonline.ca/stories/article/556011_the_arctic

_is_a_long_way_from_canadas_search_and_rescue_techs/. The original article indicated that Trenton, Ontario, was closer to Quito, Ecuador, than to Nunavut, but that distance was calculated via "flat-earth" Mercator maps. Plots using Google Earth extend the distance to a line just below Panama, bisecting Venezuela and through the northern part of Colombia.

26. Michelle Zilio, "Someday 'Your Number Is Going to Come Up': Lagging Arctic SAR Risks Much; Experts," iPolitics, 3 January 2013, http://www.ipolitics.ca/2013/01/03/someday-your-number-is-going-to-come-up-lagging-arctic-sar-risks-much-experts/.

27. Lt Jill Strelieff, "Canadian Forces High Arctic Operation Furthest Northern Patrol for Canadian Rangers" (national defense and Canadian Forces news release), Marketwired, 26 April 2010, http://www.marketwire.com/press-release/canadian-forces-high-arctic-operation-furthest-northern-patrol-for-canadian-rangers-1153921.htm.

28. This is the distance from a point in the Beaufort Sea off Canada's Yukon Territory to Nanisivik, near the entrance of Baffin Bay on Canada's east coast via Parry Sound and the McClure Strait. Using the shallower passage via the Union Strait reduces the sailing distance to approximately 900 nautical miles. See Byers and Webb, *Titanic Blunder*, map insert. Using the Norwegian model, one reckons the Northwest Passage to be 2,400 kilometers.

29. "JHC Navigating Limits Sub-Committee: Recent Incidents, 29.8.2010, Cruise Ship Runs Aground in Canadian Arctic," Lloyd's Market Association, accessed 8 August 2013, http://www.lmalloyds.com/Web/Market%20Places/_nbsp__nbsp_Marine/Joint_Hull/Navigating_Limits/Web/market_places/marine/JHC_Nav_Limits/Navigating_Limits_Sub-Committee.aspx.

30. *Nuuk Agreement*, appendices 1, 2, and 3, respectively. Joint Rescue Coordination Center–Juneau (USCG D17 RCC), staffed by the Coast Guard, is responsible for the SAR region corresponding to the panhandle of Alaska, the Aleutian chain, and the waters off the Alaska coast. The Alaska RCC is an Air Force mission encompassing the land mass of the Alaska mainland north of 58 degrees north latitude and west of 141 degrees west longitude. See "Frequently Asked Questions," Joint Base Elmendorf–Richardson, accessed 13 August 2013, http://www.jber.af.mil/shared/media/document/AFD -120314-029.html.

31. David Perera, "Papp: Coast Guard Plans No Arctic Shoreside Infrastructure," Fierce Homeland Security, 22 May 2013, http://www.fiercehomelandsecurity.com/story/papp-coast-guard-plans-no-arctic-shoreside-infrastructure/2013-05-22.

32. Coast Guard aviation assets were slashed by 92.24 percent in the House Appropriations Committee's markup for fiscal year 2014. Overall, the Coast Guard's FY 2014 budget request was cut by more than 13 percent over the previous year. David Perera, "2014 Budget Request: Coast Guard," Fierce Homeland Security, 11 April 2013, http://www.fiercehomelandsecurity.com/node/89222/print.

33. A third US-owned icebreaker does exist, but it isn't part of the Department of Defense or even Homeland Security. The National Science Foundation will have its own light-duty icebreaker, the *Sikuliaq*, in 2014, earmarked for scientific missions in the Gulf of Alaska and southern Bering Sea. House, *Testimony of Dr. Kelly Falkner, Deputy Director, Office of Polar Programs, National Science Foundation, before the House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation*, 112th Cong., 1st sess., 1 December 2011, http://www.nsf.gov/about/congress/112/kf_coastguard arctic_111201.jsp. See also ABS Consulting, *United States Coast Guard High Latitude Region Mission Analysis Capstone Summary* (Arlington, VA: ABS Consulting, July 2010), 15, http://assets.fiercemarkets.com/public/sites/govit/hlssummarycapstone.pdf. See also Ronald

O'Rourke, *Coast Guard Polar Icebreaker Modernization: Background and Issues for Congress*, CRS Report for Congress RL 34391 (Washington, DC: Congressional Research Service, 24 July 2013), "Summary," http://www.fas.org/sgp/crs/weapons/RL34391.pdf.

34. O'Rourke, *Polar Icebreaker Modernization*, 9. The Coast Guard needs several more icebreakers beyond the 3 + 3 model to achieve a continuous presence in the Arctic and the Antarctic.

35. US Coast Guard, *United States Coast Guard Arctic Strategy* (Washington, DC: Headquarters US Coast Guard, May 2013), 31–32, https://www.hsdl.org/?view&did=736969. The strategy calls for "force multipliers" under a "whole of government" approach to the Arctic.

36. Task Force Climate Change / Oceanographer of the Navy, *U.S. Navy Arctic Roadmap* (Washington, DC: Department of the Navy, October 2009), 11, 14, 17, http://www.navy.mil/navydata/documents/USN_artic_roadmap.pdf. The *Roadmap* calls for a review of existing agreements with the Air Force, among others, but nowhere does it solicit that service for additional support. The Navy's study refers to the Army more than it does the Air Force.

37. Task Force Climate Change / Oceanographer of the Navy, *U.S. Navy Arctic Roadmap*, 11, 23. The US Coast Guard's *Arctic Strategy* (see note 35) mentions its SAR obligations and the requirement for burden sharing with other Arctic nations but only touches on any future strategy. It may forward-deploy assets to Barrow, Alaska, in the summer months. Other than planning for more icebreakers to aid in SAR, the *Strategy* is silent regarding future plans.

38. In testimony before Congress, Alaska's lieutenant governor called the 176th "America's front-line for search and rescue in the Arctic Ocean," observing that "Coast Guard response is based much further away." House, *"America is Missing the Boat," Statement for the Record, the Honorable Mead Treadwell, Lieutenant Governor, State of Alaska, before the United States House of Representatives Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation*, 112th Cong., 1st sess., 1 December 2011, 9, http://housemajority.org/joule/pdfs/27/hjr0034_treadwell_testimony.pdf.

39. To put it mildly, command and control of these assets is confusing, but unity of command is a separate issue from a lack of vision regarding use of Air Force SAR assets in the High North. For a full discussion of command and control issues and recommendations for change, see Peter Ohotnicky, Braden Hisey, and Jessica Todd, "Improving U.S. Posture in the Arctic," *Joint Force Quarterly*, issue 67 (4th Quarter 2012): 56–62, http://www.ndu.edu/press/lib/pdf/jfq-67/JFQ-67_56-62_Ohotnicky-Hisey-Todd.pdf.

40. Task Force Climate Change / Oceanographer of the Navy, *U.S. Navy Arctic Roadmap*, 25, action item 5.11.

41. "RQ-4 Global Hawk," fact sheet, US Air Force, 16 October 2008, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104516/rq-4-global-hawk.aspx. This profile assumes a nominal range of 2,500 nautical miles, flown from Eielson AFB.

42. Department of Defense, *Report to Congress on Arctic Operations and the Northwest Passage*, OUSD (Policy) (Washington, DC: Department of Defense, May 2011), 14, http://www.defense.gov/pubs/pdfs/tab_a_arctic_report_public.pdf.

43. The following year, NORTHCOM's commander designated Alaska a "key focus area" and identified deficiencies in several areas, including SAR-enabling capabilities.

44. For a view of the rise of commercial maritime traffic between the West Coast of Greenland and Canada adjacent to the Northwest Passage, see Jane Kokan, "Greenland:

Canada's Arctic Neighbour," *FrontLine Defence* 9, no. 1 (January/February 2012): 23–27, http://www.frontline-canada.com/downloads/12-1_RAdmKudsk.pdf.

Col John L. Conway III, USAF, Retired

Colonel Conway (BA, MA, University of Alabama) is a military defense analyst at the Air Force Research Institute (AFRI), Maxwell AFB, Alabama. During his more than 30 years in the Air Force, he served as an intelligence officer with major assignments at Headquarters Air Intelligence Agency, North American Aerospace Defense Command, and the National Security Agency. He was the senior intelligence officer at Headquarters Air Force Reserve Command (AFRC), Robins AFB, Georgia, and held several wing and squadron intelligence assignments, including a combat tour at the II Direct Air Support Center in Pleiku Province, Republic of Vietnam, and as chief, Counterdrug Support Division, Headquarters AFRC. After retiring from active duty in 2001, Colonel Conway was a civilian adviser to the commander, Gordon Regional Security Operations Center, Fort Gordon, Georgia, following 9/11 and later was a systems engineering and technical assistance contractor to the U-2 Directorate at the Warner Robins Air Logistics Center, Robins AFB, Georgia. He is a frequent contributor to *Air and Space Power Journal*.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

Disclaimer

The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

http://www.airpower.au.af.mil

Cyberspace Superiority

A Conceptual Model

Lt Col William D. Bryant, USAF

The Airman seeks air superiority; the Sailor, maritime superiority. Does cyberspace superiority exist? Currently we have no clear consensus regarding that question. Some authors, such as RAND's cyber expert Martin Libicki argue that "cybersupremacy is meaningless and, as such, is not a proper goal for operational cyberwarriors."[1] The US Air Force disagrees, identifying cyberspace superiority as a key concept. According to Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, cyberspace superiority represents "the operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference."[2] Joint doctrine takes the middle ground. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, includes definitions for air, maritime, and space superiority but not cyber superiority. To confuse the issue further, it notes that full-spectrum superiority is the "cumulative effect of dominance in the air, land, maritime, and space domains and information environment (which includes cyberspace)."[3] Much of the confusion over cyberspace superiority stems from the difficulty of intuitively grasping what it looks like. This article seeks to overcome this difficulty by proposing a conceptual model of how cyberspace superiority works.

By its very nature, a model is not the thing itself and is significantly simplified to facilitate comprehension and analysis. However, to be useful, the model must have sufficient fidelity, and any proposed model in strategy must account for the dynamic nature of strategy whereby "the enemy gets a vote" and both sides make decisions in response to each other. Carl von Clausewitz captured this interaction in his analogy of two struggling wrestlers, each attempting to throw the other.[4] The model must do the same.

We must also note that the cyberspace superiority discussed here has to do with conflicts between nation-states. Although "hacktivists" and cyber criminals utilize some of the same tools and techniques as nation-state attackers, they have fundamentally different objectives, and their operations are not "the continuation of politics by different means."[5] In nation-state conflict, cyberspace is generally considered a global common, much like the sea, and its normal state is not to be commanded or controlled by any party.[6]

Cyberspace superiority is not an end in itself; winning the battle for such superiority does not necessarily equate to winning the overall conflict—but it certainly makes it easier. Combatants will not feel the most important effects of cyberspace superiority in cyberspace but in the other war-fighting domains. Those who operate in the land, air, maritime, and space domains rely heavily on cyberspace to carry out their missions, and a modern military would have considerable difficulty operating effectively without its information systems. To convey what cyberspace superiority means and how control of cyberspace can produce desired effects in other domains, the article builds a model reflecting the production of superiority in the air domain.

A Model of Domain Control

Because of the difficulty of comprehending something not purely physical, such as cyberspace, we begin by building a model of domain control in a more familiar environment (fig. 1). Specifically, the literature includes a great deal of discussion about air superiority, and one can examine numerous wars and case studies to determine the characteristics, elements, and interactions pertaining to the air domain. Notably, the model developed here deals only with "means" (what produces superiority in the domain) and "ways" (what those means can do both in and out of the domain). The means are the tools, and the ways are what can be done with those tools. The model remains silent regarding how those ways may or may not contribute to the overall ends of the strategy.

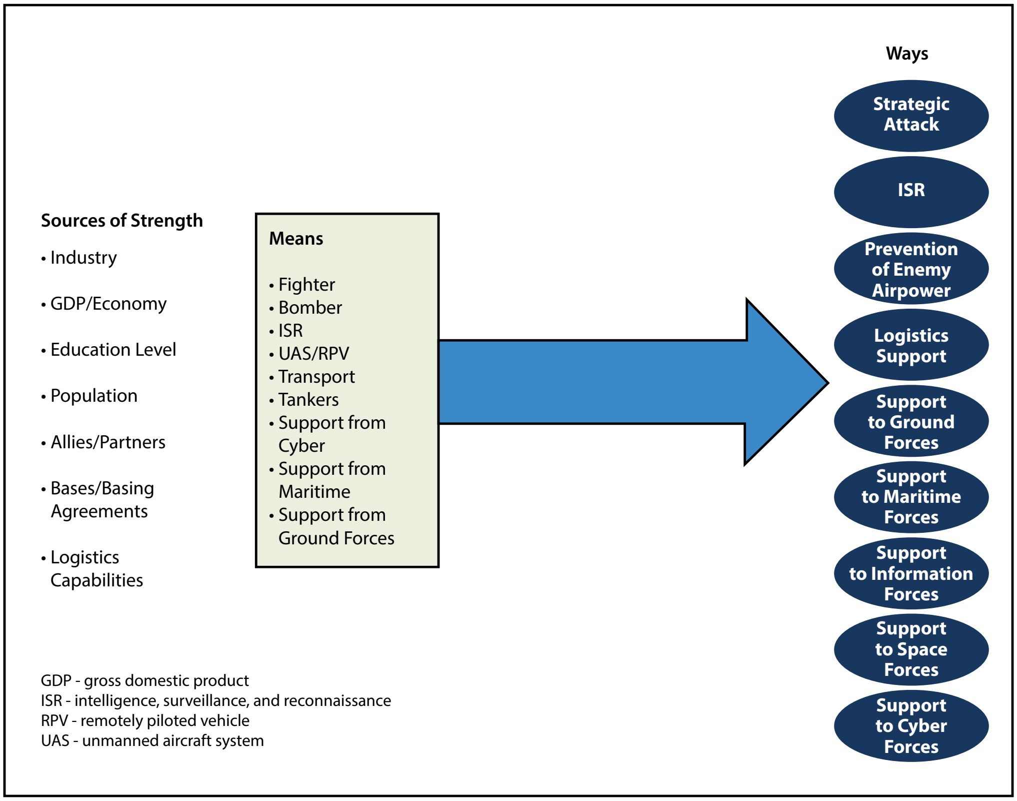


Figure 1. The means and ways of air superiority

A nation's sources of strength, such as industry and population, produce its airpower means (e.g., fighters, bombers, and tankers). The country then uses these means against an enemy to generate the airpower ways—the things that airpower can do—such as conduct strategic attack or support ground forces. However, as Clausewitz observed, "In war, the will is directed at an animate object that *reacts*" (emphasis in original).[7] The enemy will not sit idly by during an attack but will try to prevent the opponent from utilizing his means. Figure 2 depicts some of the more common ways an enemy can employ to block airpower.

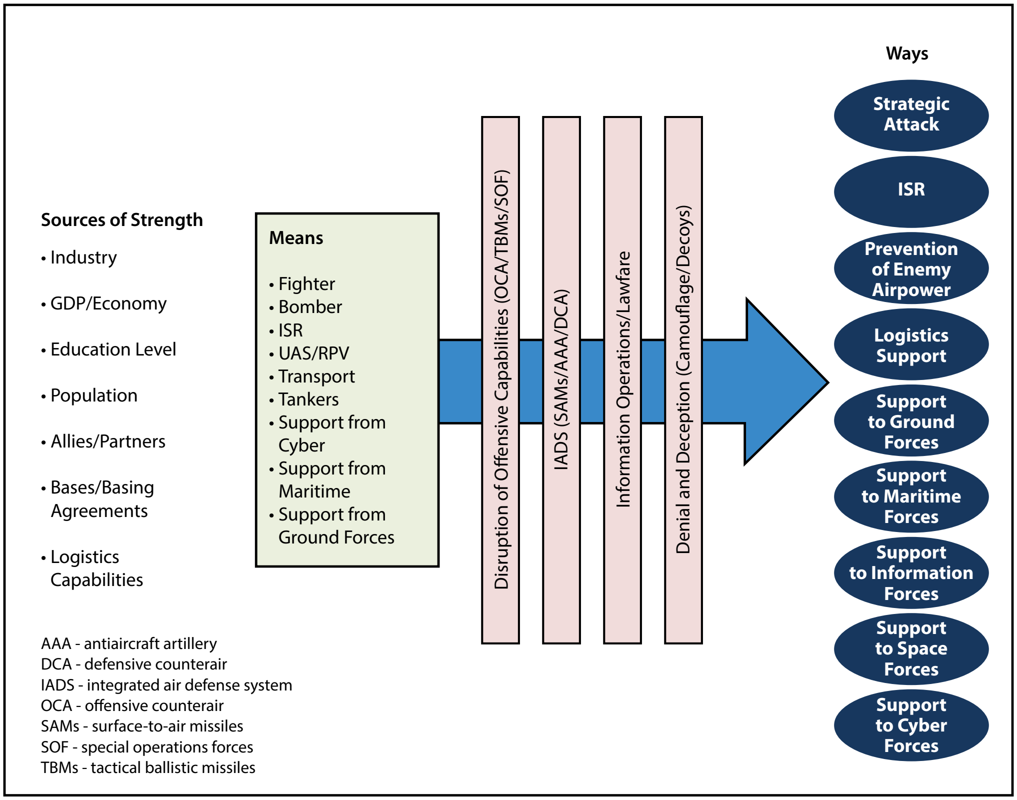

Sources of Strength
• Industry
• GDP/Economy
• Education Level
• Population
• Allies/Partners
• Bases/Basing Agreements
• Logistics Capabilities
Means
• Fighter
• Bomber
• ISR
• UAS/RPV
• Transport
• Tankers
• Support from Cyber
• Support from Maritime
• Support from Ground Forces
Disruption of Offensive Capabilities (OCA/TBMs/SOF)
IADS (SAMs/AAA/DCA)
Information Operations/Lawfare
Denial and Deception (Camouflage/Decoys)
Ways
Strategic Attack
ISR
Prevention of Enemy Airpower
Logistics Support
Support to Ground Forces
Support to Maritime Forces
Support to Information Forces
Support to Space Forces
Support to Cyber Forces
AAA - antiaircraft artillery
DCA - defensive counterair
IADS - integrated air defense system
OCA - offensive counterair
SAMs - surface-to-air missiles
SOF - special operations forces
TBMs - tactical ballistic missiles

Figure 2. The means and ways of air superiority with adversary blocking

However, the dynamic nature of strategy, in which every action generates a reaction from the enemy, has not yet concluded. The initiator of the action can also react to the enemy's action by bringing into play a number of well-known and potentially effective measures. Figure 3, the complete model of air superiority, illustrates some of the attacker's potential mitigation strategies.

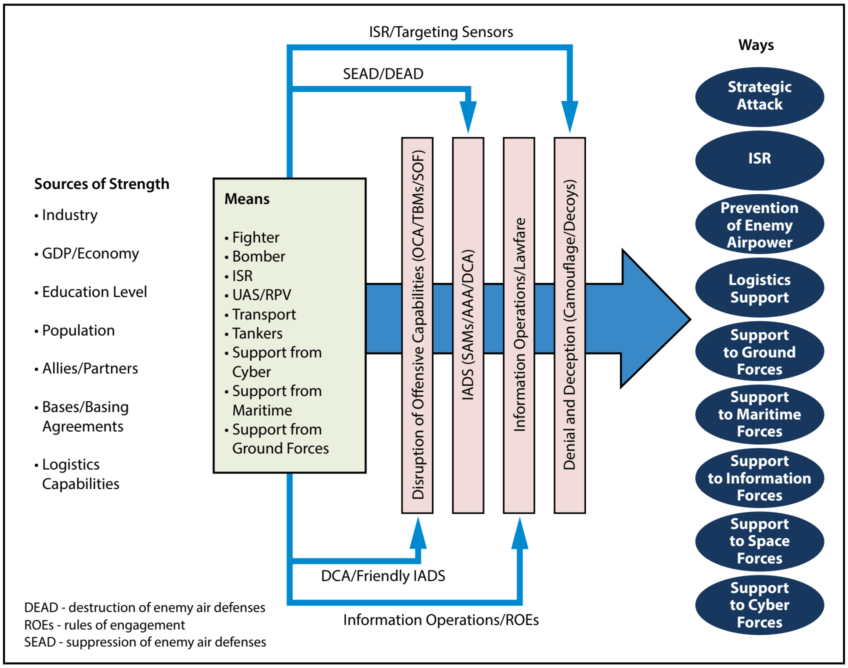

ISR/Targeting Sensors
SEAD/DEAD
Ways
Strategic Attack
ISR
Prevention of Enemy Airpower
Logistics Support
Support to Ground Forces
Support to Maritime Forces
Support to Information Forces
Support to Space Forces
Support to Cyber Forces
Sources of Strength
• Industry
• GDP/Economy
• Education Level
• Population
• Allies/Partners
• Bases/Basing Agreements
• Logistics Capabilities
Means
• Fighter
• Bomber
• ISR
• UAS/RPV
• Transport
• Tankers
• Support from Cyber
• Support from Maritime
• Support from Ground Forces
Disruption of Offensive Capabilities (OCA/TBMs/SOF)
IADS (SAMs/AAA/DCA)
Information Operations/Lawfare
Denial and Deception (Camouflage/Decoys)
DCA/Friendly IADS
Information Operations/ROEs
DEAD - destruction of enemy air defenses
ROEs - rules of engagement
SEAD - suppression of enemy air defenses

Figure 3. Air superiority model

Of course, reactions to reactions may go on ad infinitum, but moving only two levels up is sufficient to make the dynamic nature of the contest apparent. The model shows elements the initiator needs to strengthen, options the enemy has to block him, and choices for weakening those blocks along with the ways available to the initiator. All of this is relatively uncontroversial in the air domain, but the unique characteristics of the cyber domain lead to very different elements in the model.

Unique Characteristics of the Cyberspace Domain

Building a model of cyberspace superiority requires accounting for the distinctive characteristics of the cyberspace domain. Because the domain is man-made (the first characteristic), its geography is always subject to change by the combatants or third parties. Gregory Rattray, author of *Strategic Warfare in Cyberspace*, remarks that "cyberspace is unique in that the interactions are governed by hardware and software that is manmade, so the 'geography' of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the flick of a switch; they can be created or 'moved' by insertion of new coded instructions in a router or switch."[8] This mutability goes beyond the ability to move "geographical" features; we can also copy the rivers, mountains, and oceans of cyberspace; store them at will; and reinsert them later if the need arises. As data-storage costs continue to plummet, it becomes ever more practical for combatants to have multiple copies of everything. Libicki maintains that since cyberspace is replicable, it is also repairable—a notion that has significant implications for the persistence of effects in cyberspace.[9]

As is the case with the air and maritime domains, combatants access cyberspace via technology but at far less cost. The ports and ships of the maritime domain as well as the aircraft and airfields of the air domain demand an immense expenditure of resources generally available only to nation-states. In contrast, the port or airfield of cyberspace is as close as the nearest Internet service provider or Internet café, and the delivery vehicle for an attack can be a simple laptop purchased nearly anywhere for less than $500. Significant capability can prove extremely resource intensive and take years to develop, but the initial cost of entry remains quite low. Furthermore, the resources necessary for success ordinarily take the form of highly trained and competent personnel as opposed to major expenditures in infrastructure and equipment.

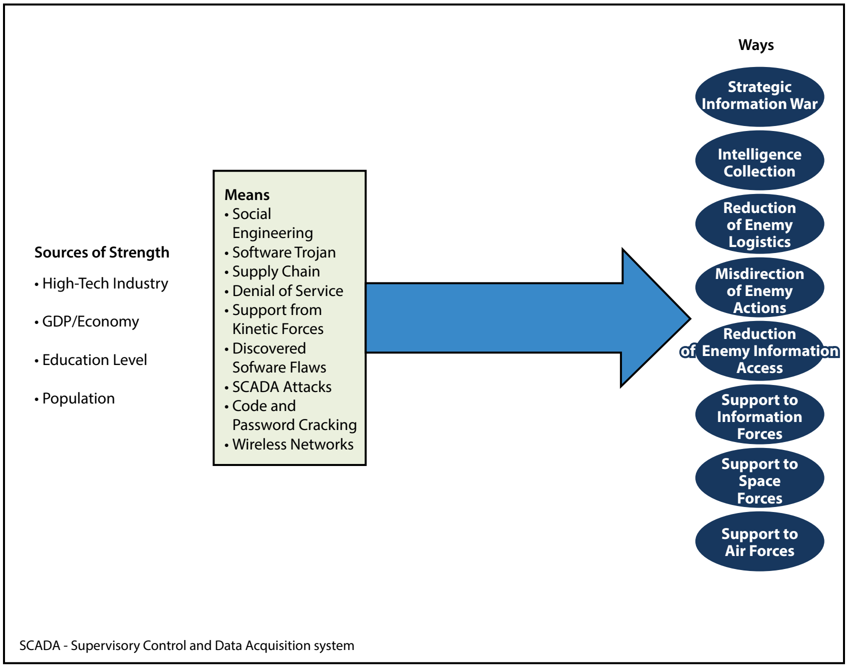
We must also recognize that control of cyberspace is unlikely to win the war by itself. Although the uncertainty generated by the enemy's knowledge that the opponent can manipulate his information systems can be important, it probably won't make him give up the objectives he was willing to fight for in the first place. Possession of land can prove significant—possession of cyberspace less so. However, cyberspace superiority allows us to do things with the information resident in cyberspace and to produce effects in other domains through cyberspace. For example, the fact that an enemy can access a US logistics system is noteworthy because he could obtain information that shows where forces are going and could manipulate the system to make those forces less effective in other domains by reducing their supplies. The fact that an adversary has hacked into the control system of a power plant has significance because of the effect he could generate in other domains by affecting the power plant through cyberspace.

Another characteristic of cyberspace, the asymmetry between offense and defense, also applies to some extent in the air domain since an asymmetry exists between offensive airpower and ground-based defenses in modern air combat. A modern integrated air defense system utilizes surface-to-air missiles, antiaircraft artillery, fighters, and surveillance assets integrated with command and control. With the exception of multirole fighters, these defenses cannot perform offensive missions into enemy territory; they can only target incoming aircraft. A similar asymmetry exists between the defense and offense in cyberspace, where defensive and offensive systems are neither similar nor interchangeable. This asymmetry contrasts the situation in sea warfare, in which a destroyer can operate either offensively or defensively, much like a tank or an infantryman. A firewall and a worm, important elements of cyberspace, are fundamentally different and no more interchangeable than a Patriot missile and a B-52.

Because they rely on deception for access, cyberspace weapons are extremely frangible. Like glass swords, they can be sharp and lethal but may break on the first swing. Upon recognizing an enemy exploit, the defender will engineer patches to stop further attacks that use the same opening. Additionally, like glass swords, cyberspace weapons are difficult to detect. Cyberspace offensives that utilize unknown, exploitable flaws are referred to as "zero day" attacks because the timer on the vulnerability starts at zero when the first strike occurs and then rises in increments as software engineers scramble to develop a patch. Defenders unaware of the specific vulnerability rely on systems that look for generic signatures—often with only moderate success. Thus they consider zero-day exploits important and guard against them carefully after discovery. Given these characteristics, we can now build a model of cyberspace superiority.

Cyberspace Superiority Model

Employing some concepts from the other domains as well as the characteristics of cyberspace, figure 4 presents the means and ways of cyberspace.



SCADA - Supervisory Control and Data Acquisition system

Figure 4. The means and ways of cyberspace superiority

Cyber Means

A nation's cyberspace sources of strength produce the capabilities or means currently available in cyberspace. By means of social engineering, the attacker convinces users to unknowingly take some action that lets him into the system. He can also develop software "Trojan horses" or strike an enemy supply chain where some sort of access port or capability is manufactured into either the software or hardware used by the defender. Additionally, the enemy may utilize denial-of-service attacks, overwhelming a defender's systems with so many false requests for information that they cannot function effectively. He may physically take apart an information system by some kinetic means, whether a Joint Direct Attack Munition dropped by a fighter or a pack of C4 plastic explosive delivered by a special operator. Cross-domain effects can proceed both from the physical world to cyberspace and vice versa. Discovered software flaws are the "crown jewels" of any attacker's arsenal because they allow him to develop specific strikes to gain access and carry out his intent. Such flaws are useful in inverse relation to the information technology community's familiarity with them. Generally, defenders can quickly produce a patch for a widely known problem and begin to close the attacker's window of opportunity. It normally does not close completely since many users and system administrators fail to patch their systems properly, but conducting an attack becomes much more challenging.

A special category of cyber attacks targets Supervisory Control and Data Acquisition systems, which operate infrastructure such as power plants, dams, water-treatment facilities, and so forth. Alarmists usually cite these systems when they want to make apocalyptic predictions of cyberspace attacks to generate funding from Congress. In theory, such a strike could shut down almost any modern system. Depending on the specific system under attack, sometimes an adversary can do far more damage than he can by simply turning something off that the defender can immediately turn on again. For example the Stuxnet worm, which can carry out a very sophisticated assault on a control system, allegedly caused the physical destruction of components while reporting that all was well to the system's engineers.[10] Further, code and password cracking can facilitate entry or retrieve information, and wireless networks provide another potential port of entry for attackers—even into "air-gapped" systems (those not directly plugged into the broader Internet).

Cyber Ways

These means can accomplish a number of different ways in pursuit of strategic end states. First, an attacker can use them in strategic information warfare, during which a nation uses cyberspace to directly attack centers of gravity. According to Maj Eric Trias and Capt Bryan Bell, "The goal of strategic attack is to apply force systematically against enemy centers of gravity in order to produce the greatest effect for the least cost in dollars and lives."[11] Just as bombers strike a city to punish civilians and convince them to pressure their government to change its policy, so would a cyberspace attack inhibit or destroy the infrastructure of a city in an attempt to produce the same effect.

The majority of cyberspace intrusions by nation-states during peacetime appear focused on intelligence gathering and cyber espionage, which also has great importance during a conflict. Examples include breaking into an enemy's system to read his war plans or check on the readiness of his forces or capabilities.

Attackers can choose to launch their assaults against enemy logistics systems. Modern militaries rely on their information systems for logistical support; because multiple users in various locations must access these systems, they are often on unclassified networks and open to attack. Misdirection that sends supplies to the wrong places, changes inventory information, or alters timetables could have a tremendous impact on a campaign, particularly if the enemy relies heavily upon moving large numbers of forces a great distance in a short period of time. Obviously, the United States is especially vulnerable in this area.

Reducing the enemy's access to information will lessen the effectiveness of his forces. A more subtle approach involves misdirecting him and shaping his actions by altering his picture of what is happening around him. This technique can include false information, but the availability of multiple sources of data can hinder its success. Such an approach generally works best when it reinforces something the enemy is inclined to believe anyway—witness the operation to convince Hitler that the Allies would land at Calais, not Normandy. Rather than use false data, these attacks can employ technically true information to build a misleading picture. The attacker seeks to shape the decision space around the enemy to make him more likely to do something he wants him to do.

Cyberspace also provides critical support to all of the other warfighting domains.[12] For instance, a cyberspace attack could fool an enemy's integrated air defense system into not seeing an airborne strike package or could disable his space jamming system. As is the case with airpower, though, the enemy probably will not endure these actions passively but will try to block them (fig. 5).

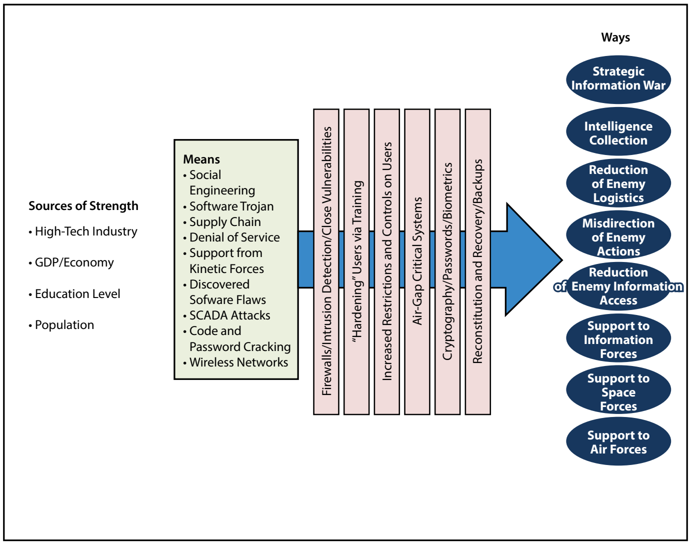

Sources of Strength
• High-Tech Industry
• GDP/Economy
• Education Level
• Population
Means
• Social Engineering
• Software Trojan
• Supply Chain
• Denial of Service
• Support from Kinetic Forces
• Discovered Sofware Flaws
• SCADA Attacks
• Code and Password Cracking
• Wireless Networks
Firewalls/Intrusion Detection/Close Vulnerabilities
"Hardening" Users via Training
Increased Restrictions and Controls on Users
Air-Gap Critical Systems
Cryptography/Passwords/Biometrics
Reconstitution and Recovery/Backups
Ways
Strategic Information War
Intelligence Collection
Reduction of Enemy Logistics
Misdirection of Enemy Actions
Reduction of Enemy Information Access
Support to Information Forces
Support to Space Forces
Support to Air Forces

Figure 5. The means and ways of cyberspace superiority with defensive blocks

Cyber Defensive Blocks

Defenders can utilize a number of methods to protect themselves from cyberspace attacks. One of the most common entails preventing unauthorized access by installing firewalls, intrusion detection, and authentication systems. Closing known vulnerabilities is also critical since many systems do not have the latest patches.

Users are the bane of system administrators the world over, and many attacks rely on finding individuals who can be tricked into doing something that they should not. Because most users have only a rudimentary knowledge of computer security, the time and money spent on training them can produce a significant payoff.

Systems administrators can also decrease the risk posed by users by increasing restrictions and controls, but reducing connectivity can come at a substantial cost. Information systems exist to process and share information; if overzealous administrators can be convinced to shut off systems from the outside world, they may give the attacker exactly what he wants because such an action significantly reduces capability. Defenders must find the right balance between access and security so that they can avoid doing the attacker's work for him.

Moreover, defenders can air-gap (disconnect) systems from direct access to the Internet—an appropriate action for highly sensitive and critical systems such as those associated with nuclear weapons. Airgapping offers no guarantee against attack, however, since a clever adversary may find other methods of access. Options include physical access to the system, enabled wireless-networking capabilities, and mistakes by users who inadvertently connect the air-gapped system into the wider Internet.

A system may also continue to use the backbone of the Internet while relying on encryption to keep information out of unfriendly hands. The use of passwords is standard practice now on most systems as a means of denying attackers access to them. Furthermore, if implemented properly, biometric identification or token identification such as common access cards can help keep intruders out of systems.

A final way of blocking attackers makes use of backups and resiliency. Despite the media attention given to major worms such as Melissa or Slammer, most information technology operations recovered fully in a couple of days.[13] An attacker who penetrates all defenses and completely erases the data in a logistics system can cause severe problems for defenders. If the latter have a backup on removable media that the attacker did not know about or could not access and if they can have the system up and running in a day, then the effects of the strike may prove minimal. The completed cyberspace superiority model illustrates several methods that the attacker can use to reduce the effectiveness of these attempted blocks (fig. 6).

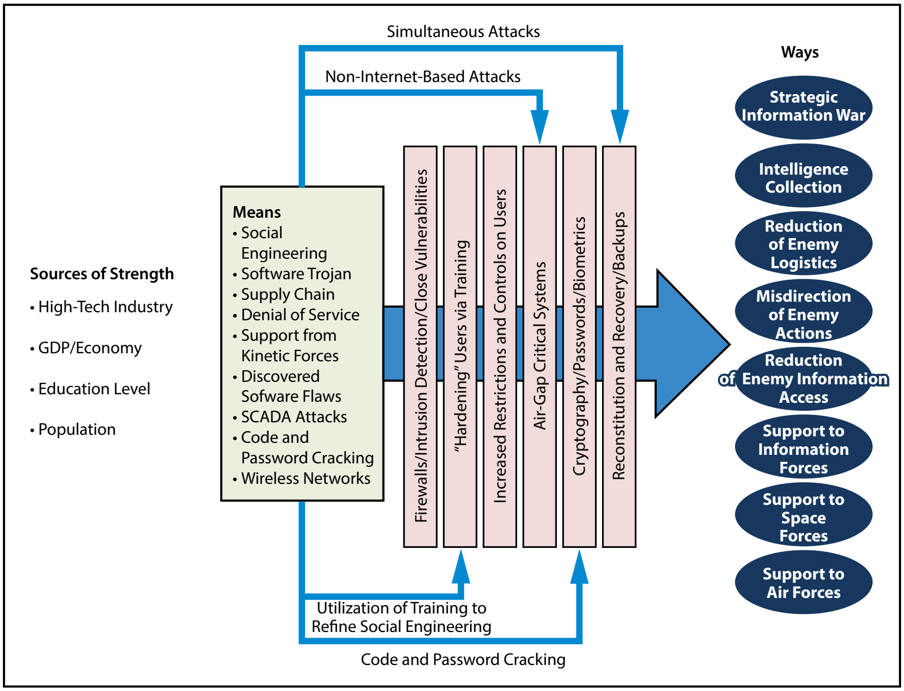

Simultaneous Attacks
Non-Internet-Based Attacks
Ways
Strategic Information War
Intelligence Collection
Reduction of Enemy Logistics
Misdirection of Enemy Actions
Reduction of Enemy Information Access
Support to Information Forces
Support to Space Forces
Support to Air Forces
Sources of Strength
• High-Tech Industry
• GDP/Economy
• Education Level
• Population
Means
• Social Engineering
• Software Trojan
• Supply Chain
• Denial of Service
• Support from Kinetic Forces
• Discovered Sofware Flaws
• SCADA Attacks
• Code and Password Cracking
• Wireless Networks
Firewalls/Intrusion Detection/Close Vulnerabilities
"Hardening" Users via Training
Increased Restrictions and Controls on Users
Air-Gap Critical Systems
Cryptography/Passwords/Biometrics
Reconstitution and Recovery/Backups
Utilization of Training to Refine Social Engineering
Code and Password Cracking

Figure 6. Cyberspace superiority model

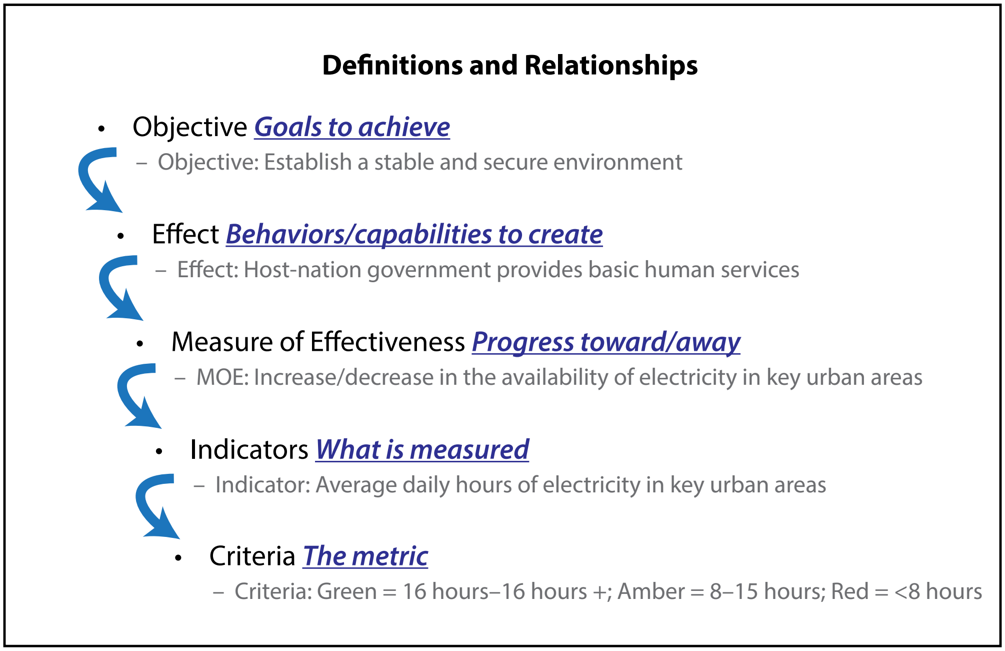
Cyber Attackers' Counters to Defensive Blocks

If the enemy carefully examines the defender's training program, he can refine his social engineering to focus on methods not covered in the training or on those similar to training examples deemed acceptable. Just one user making a mistake can open a window of opportunity. Adversaries can use non-Internet-based attacks to access air-gapped systems—perhaps by way of a wireless modem inadvertently left out or turned on, insertion of malicious code in the defender's supply chain, or physical access to the system through espionage or special operations. Moreover, code and password cracking can defeat encryption, particularly if a clever attacker finds a technique to access the encryption keys so that he does not have to resort to brute force. Finally, an adversary can use simultaneous strikes to go after backup as well as primary systems to prevent easy copying of data as a means of protection. Although Internet hoaxes about viruses that can melt computers into a puddle of goo are overstated, it may be possible to attack the hardware itself and thus increase the amount of time necessary to recover functionality.

This model will not remain static; rather, it will change with newly developed techniques and procedures. As with the airpower model, new technology will produce new capabilities for both the offense and defense. Each side maneuvers in relation to what the other does, and Clausewitz's wrestling match will continue.

Measurement of Cyberspace Superiority

Testing of the proposed model requires specific metrics, such as those developed by US Joint Forces Command (fig. 7). In the figure, the lower levels feed into the higher ones, and it is important to note the possibility of multiple indicators for each measure of effectiveness (MOE), multiple MOEs for each effect, and multiple effects for each objective. Further, depending on the situation, there may be only one effect per objective, and so forth.



Definitions and Relationships

- Objective *Goals to achieve*
  - Objective: Establish a stable and secure environment
- Effect *Behaviors/capabilities to create*
  - Effect: Host-nation government provides basic human services
- Measure of Effectiveness *Progress toward/away*
  - MOE: Increase/decrease in the availability of electricity in key urban areas
- Indicators *What is measured*
  - Indicator: Average daily hours of electricity in key urban areas
- Criteria *The metric*
  - Criteria: Green = 16 hours–16 hours +; Amber = 8–15 hours; Red = <8 hours

Figure 7. Effects component summary. (Adapted from Department of Defense, US Joint Forces Command, "Tactics, Techniques, and Procedures: Assessment of Joint Operations," 10 March 2008, I-6, fig. I-3.)

Cyberspace superiority will be local and transient. In accordance with the definition in AFDD 3-12, mentioned previously, when a friendly force can "conduct operations at a given time and in a given domain without prohibitive interference," it has attained cyberspace superiority. Such superiority is not global and comprehensive; it is relative to what the attacker in a conflict attempts to accomplish. In the cyberspace model suggested in figure 6, the objective or goal is the way that the attacker seeks. For example, an adversary might want to reduce his enemy's logistical capability by producing the desired effect of immobilizing the enemy's armored forces due to a lack of supplies. The attacker's corresponding MOE could involve a change in the supply status of enemy armored divisions, indicated by the level of supply possessed by specific divisions in the regular categories of supply. The following could serve as a metric for an attacker: for a specific enemy division, green represents fuel reserves of 24 hours or fewer; amber, 24–72 hours; and red, more than 72 hours.

The cyber component in the above example could entail a concentrated attack on the enemy's computerized logistical system to misdirect fuel away from the divisions that the attacker intends to engage. This overly simplistic example illustrates several important issues with measuring cyberspace superiority. First, an attacker probably would not rely solely on cyberspace strikes to decrease the enemy's fuel supply but use other kinetic means as well. The fact that the armored division is out of fuel does not mean that cyberspace operations are responsible. Perhaps the attacker also wrecked bridges, hit fuel dumps, and destroyed the defender's fuel trucks. Since combat situations are not repeatable, it is not possible to run a campaign, note the outcome, and then reset and conduct the same campaign again without utilizing cyberspace attacks to determine whether a difference exists.

Applying the Model

The cyber attack on Aramco, which occurred in 2012, offers an example of how we can apply this model to a real case. Some of the details remain murky and highly classified by the various governments involved, but open-source literature includes sufficient information to justify an examination of this incident. According to the *New York Times*, the attackers—who claimed to belong to an activist group called the Cutting Sword of Justice—were attempting to shut down Aramco's production of oil and natural gas.[14] US intelligence officials, however, maintain that Iran orchestrated the attack in retaliation for the Stuxnet attack on its nuclear program.[15] In the cyberspace superiority model, the attacker's way involved the use of strategic information warfare and cyberspace attack to directly affect a physical target. Evidently, the selected means called for social engineering and a "spear phishing" attack.[16]

More specifically, the attacker sought to shut down Aramco's production of oil and natural gas and wished to produce the desired effect of halting its production. The MOE was a change in that production, indicated by the amount of oil and natural gas produced by Aramco. Although we do not know the attacker's criteria, we can use the following example: less than 50 percent production = green, 50–75 percent = amber, and 75–100 percent = red. In this case, it is easy to determine whether or not the attacker attained cyberspace superiority because despite affecting 30,000 computers, the strike did not reduce production at all.[17] By utilizing the cyberspace superiority model, we can clearly see why the attack proved unsuccessful. Specifically, because Aramco segregated its office computers from those that controlled oil and gas production, the attack could not get past the air gap. Figure 8 illustrates the elements of the Aramco cyber attack and the successful block.

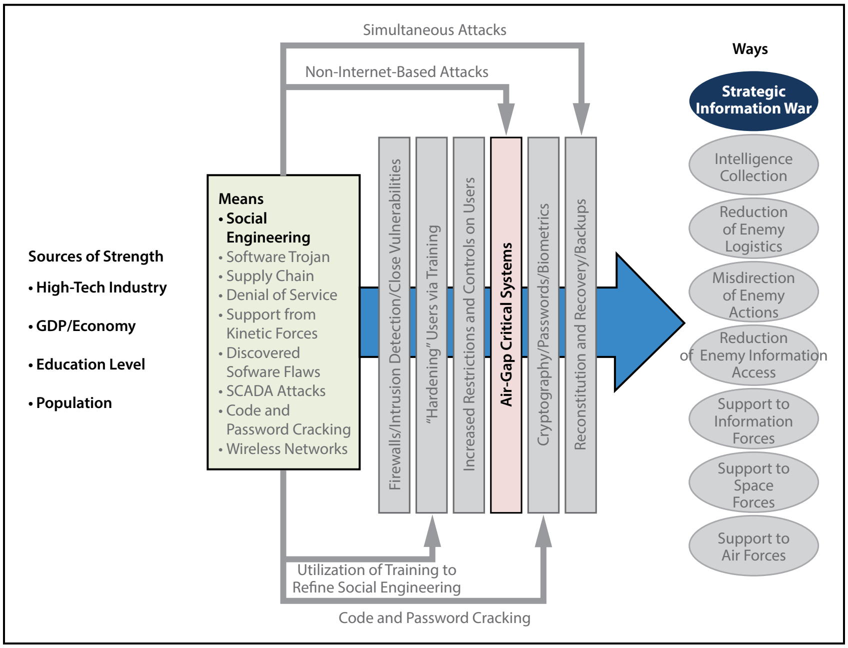

Simultaneous Attacks
Non-Internet-Based Attacks
Ways
Strategic Information War
Intelligence Collection
Reduction of Enemy Logistics
Misdirection of Enemy Actions
Reduction of Enemy Information Access
Support to Information Forces
Support to Space Forces
Support to Air Forces
Sources of Strength
• High-Tech Industry
• GDP/Economy
• Education Level
• Population
Means
• Social Engineering
• Software Trojan
• Supply Chain
• Denial of Service
• Support from Kinetic Forces
• Discovered Sofware Flaws
• SCADA Attacks
• Code and Password Cracking
• Wireless Networks
Firewalls/Intrusion Detection/Close Vulnerabilities
"Hardening" Users via Training
Increased Restrictions and Controls on Users
Air-Gap Critical Systems
Cryptography/Passwords/Biometrics
Reconstitution and Recovery/Backups
Utilization of Training to Refine Social Engineering
Code and Password Cracking

Figure 8. Aramco cyber-attack elements of the cyberspace superiority model

In this case, a successful defense prevented the attacker from attaining cyberspace superiority. This is not to say that the strike accomplished nothing at all; indeed, it inflicted a tremendous amount of damage on Aramco's systems and increased uncertainty in the Middle East. However, the attacker did not realize his stated goal of shutting down the production of oil and gas and thus could not execute operations in cyberspace without prohibitive interference.

Conclusion

This proposed model can be used to analyze cyber attacks, defenses, and the interactions between the two across multiple different types of cyber assaults. Though useful, without careful application, the model could become merely a backwards-looking measurement that includes elements of battle damage assessment and lessons learned. What we did yesterday is important—but mostly as a jumping-off point to assess what we can do tomorrow. Commanders want to know how much cyber superiority they have today, whether it is enough to do what they need to do tomorrow, and, if not, how they can get more. The proposed model can help answer these questions if we apply it deliberately in a forward-looking manner. If an air gap blocked yesterday's attacks, what can we do to find a way around that obstacle? If today's attack succeeded but the avenue became compromised and the defender has now closed it, do we have another path for tomorrow's attack? We must also add up the results across multiple objectives. If a commander has eight missions to carry out but expects success in two of them, that is not cyberspace superiority because the enemy is producing prohibitive interference. The model offers a structured way to think about superiority in the cyber domain that can help identify opportunities and risks which enable cyber warriors to better posture themselves for success.

War gamers can also use it as a template in both gaming and exercises to model the environment, as can commanders interested in looking at the defensive end of the model. Although this article emphasized cyber attack, defenders can just as easily apply the model to look at their plans to determine where they could strengthen them, always bearing in mind that the enemy will meet every action with a reaction.

The real utility in the proposed model is not that it will inform defenders that they need firewalls or alert attackers to software flaws. Everyone already has a good grasp of these concepts. Not as well understood, however, are the dynamic interactions between the various elements of cyberspace attack and defense. Clausewitz's wrestling match continues into cyberspace. This is where the proposed model has the most utility, and even though it will undoubtedly require refinement over time, it offers a useful framework for understanding the dynamics of cyberspace superiority. ✪

Notes

[1] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 141, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

[2] Air Force Doctrine Document 3-12, *Cyberspace Operations*, 15 July 2010 (incorporating change 1, 30 November 2011), 2, http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-12/afdd3-12.pdf.

[3] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 16 July 2013), 115, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[4] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

[5] Ibid., 7.

[6] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 185.

[7] Clausewitz, *On War*, 149.

[8] Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Dulles, VA: Potomac Books, [2009]), 256.

[9] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 5.

[10] Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal*, 15 April 2011, 2, http://smallwarsjournal.com/blog/journal/docs-temp/734-shakarian3.pdf.

[11] Maj Eric D. Trias and Capt Bryan M. Bell, "Cyber This, Cyber That . . . So What?," *Air and Space Power Journal* 24, no. 1 (Spring 2010): 91, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj10/spr10/aspj_en_2010_1.pdf.

[12] Shawn Brimley, "Promoting Security in Common Domains," *Washington Quarterly* 33, no. 3 (July 2010): 122, http://www.dtic.mil/cgi-bin/GetTRDoc?AD = ADA536657.

[13] Libicki, *Conquest in Cyberspace*, 37.

[14] Reuters, "Aramco Says Cyberattack Was Aimed at Production," *New York Times*, 9 December 2012, http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r = 0.

[15] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, 23 October 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted = all.

[16] Wael Mahdi, "Saudi Arabia Says Aramco Cyberattack Came from Foreign States," *Bloomberg,* 9 December 2012, http://www.bloomberg.com/news/2012-12-09/saudi-arabia-says-aramco-cyberattack-came-from-foreign-states.html.

[17] Ibid.

Lt Col William D. Bryant, USAF

Lieutenant Colonel Bryant (USAFA; MA, American Military University; MA, George Washington University; MSS [Master of Space Systems], Air Force Institute of Technology; MAAS [Master of Airpower Art and Science], School of Advanced Air and Space Studies) is a student at the Air War College at Maxwell AFB, Alabama. A former operational support squadron commander and director of operations, he has served on numerous operational and staff assignments. As a career fighter pilot, Lieutenant Colonel Bryant has more than 1,500 hours in the F-16.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

Disclaimer

The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

http://www.airpower.au.af.mil

A Strategic Assessment of Infrastructure Asset-Management Modeling

Lt Col William E. Sitzabee, PhD, PE, USAF
Capt Marie T. Harnly, USAF

Budget constraints and scarce resources have sparked agencies to maximize efficiency when operating and maintaining aging infrastructure. For example, in 2007 Air Force civil engineers introduced a formalized approach for maintaining infrastructure, labeling it asset management in order to optimize the performance of the 139,556 infrastructure assets (facilities, runways, utility lines, and roadways) valued at $263.43 billion.[1] Along with introducing asset management, the Air Force's senior leadership restructured civil engineer organizations and incorporated an asset-management function at all vertical levels to address such issues as a shrinking budget, deterioration of infrastructure, significant demand for infrastructure projects, and infrastructure challenges. Specifically, these leaders intended to balance resources across asset types, reduce the stock of infrastructure assets, and decrease the maintenance and repair budget—all the while maintaining a constant level of service and operations.[2] The incorporation of asset-management functions at all vertical organizational levels (unit, major command, and headquarters) emphasized planning and implementing asset-management principles in daily decision making. Air Force leaders introduced the culture change of this type of management into its organizations to handle infrastructure assets efficiently and maximize limited resources.[3]

The comprehensive framework necessary to provide guidance for asset-management business principles drove the need to restructure civil engineer units further and, under transformation, established the Air Force Civil Engineer Center, headquartered at Joint Base San Antonio, Texas. The next step calls for implementing a comprehensive asset-management framework that offers guidance for agencies with large, varying infrastructure sets and limited resources, such as the Air Force. This framework would illustrate relationships among the components of asset management and integrate them into a useful decision-support system. It would also optimize the performance of infrastructure assets and give decision makers the appropriate information to develop viable approaches and alternatives.[4] Thus, this article introduces a comprehensive asset-management framework for the agencies mentioned above—one that would allow them to conduct effective management of infrastructure assets. Such a framework would translate common and well-established asset-management philosophies into an implementable solution. Next-generation technology enables senior leadership to apply this asset-management framework as well as align the strategic-, operational-, and tactical-level data into an efficient decision-support system. To illustrate implementation of the comprehensive framework, its validity, and relationships among the components of asset management, this article uses a representative sample of Air Force infrastructure.[5]

Infrastructure Challenges

Four issues sparked the need for a comprehensive asset-management framework: financial factors as opposed to technical factors, short-term as opposed to long-term planning, a network as opposed to individual projects, and allocation of resources across asset types.[6] When implementing a solution, one weighs financial factors, such as cost of maintenance and repair projects, against technical factors, such as structural quality of roofs and foundations. A shrinking budget and the monetary cost of necessary projects exceeding the funds available for these projects exacerbate the constant problem of financial constraints. Under these circumstances, "asset managers must allocate funds among competing, yet deserving requirements."[7] Additionally, short-term remedies are evaluated against long-term goals. A short-term fix may not be the most economical solution, and a long-term strategy may not be the timeliest solution.[8] The difficulty in balancing short- and long-term factors significantly increases with rapidly changing targets and goals. These issues hinder the ability to assess and delineate short- and long-term budgets and priorities, creating an increasingly difficult task.

Infrastructure is an integrated system with individual components that function both independently and in conjunction with other systems.[9] The interconnectedness of infrastructure links assets into a complex system of interrelated elements.[10] This concept of infrastructure coupling correlates the state of one infrastructure asset to the state of another, creating an interdependency between the two; however, most maintenance management systems (MMS) assess only individual components or isolated projects instead of accounting for individual projects, network goals, and coupling effects.[11] These individual projects are weighed against networks in which infrastructure is constrained by the weakest link or networks whose parts demand simultaneous replacement in neighboring systems.

Last, budget constraints for maintenance and repair projects require decision makers to allocate and balance resources across asset types as they consider an asset's value to an agency's operations and the current condition of the infrastructure. The difficulty in allocating resources across numerous types of infrastructure encompasses objective comparison among these assets of their worth and importance. Rapidly evolving leadership drives altered goals along with these issues, producing an increasingly arduous task of delineating among assets and determining which ones need resource allocation. The contending factors of financial as opposed to technical; short-term as opposed to long-term planning; a network as opposed to individual projects; and allocation of resources across asset types represent challenges as well as opportunities for decision makers, bringing about the necessity of a comprehensive asset-management framework for numerous infrastructure types that properly balances these aspects and guides the analytical process of asset management.

Data-Modeling Process

Several strategic asset-management models exist (e.g., the Transportation Asset Management Guide); however, turning these frameworks into a useful decision-making tool for Air Force asset management demanded a comprehensive data model capable of implementing the service's specific requirements. Thus, the researchers used a data-modeling process developed by Paul Longley, Mike Goodchild, David Maguire, and David Rhind to build a comprehensive framework that incorporates well-understood components of asset management.[12] The method of data modeling is a type of systems modeling that defines and analyzes data requirements to support an agency's business practices.[13] Specifically, "a data model is a set of constructs for representing objects and processes in the digital environment."[14] A data model also involves ontologies, which define the components of a system and associate them in classes, relationships, or functions.[15] Data modeling consists of four levels (listed in order of increasing abstraction): reality, conceptual model, logical model, and physical model.[16]

Reality

Reality establishes an understanding of the system and the interactions of its components.[17] Furthermore, it includes aspects deemed applicable to the real-world construct.

Conceptual Model

The conceptual model, oriented toward its human users, consists of selected objects and processes relevant to the problem domain.[18] It identifies objects of significance, collects information, and describes associations between components.

Logical Model

Depicted in diagrams and lists, a logical model is an implementation-oriented representation of reality.[19] It depicts the entities, attributes, and relationships among the components of a system. The development of a logical model includes matching organizational functions with specific data necessary to support each function as well as illustrating influential strategic components.[20] This type of model assists agencies in engendering a common understanding of the business processes of asset management, data requisites, and maintenance and repair requirements across both vertical and horizontal boundaries.

Physical Model

A computer-oriented physical model portrays the actual implementation and demonstrates the digital application of objects.[21] It describes the databases and identifies the information needed for the process.[22] This type of model assists agencies in attaining efficient access to data across the enterprise as well as integrity of data and security measures.[23]

For the scope of this article, data modeling focuses on asset-management processes for agencies with large, varying infrastructure sets and the information necessary to make decisions based upon the strategic components of these infrastructure systems. Ultimately, the article seeks to evaluate the Air Force's asset management and guide the execution of next-generation information technology as a means of creating a decision-support system for agencies with substantial, assorted infrastructure inventories and limited resources.

Results: Logical Model

Development of the logical asset-management model produced a comprehensive framework of an operational infrastructure system with numerous types of assets. This logical model consists of components—defined and described in the reality-model and conceptual-model phases—prevalent to the business practices of asset management. Figure 1 presents the logical model, graphically depicting influential strategic components as well as relationships vital to the asset-management process. It also illustrates the ontologies and associations among the asset-management components and identifies the data required to promote analysis of infrastructure operations.

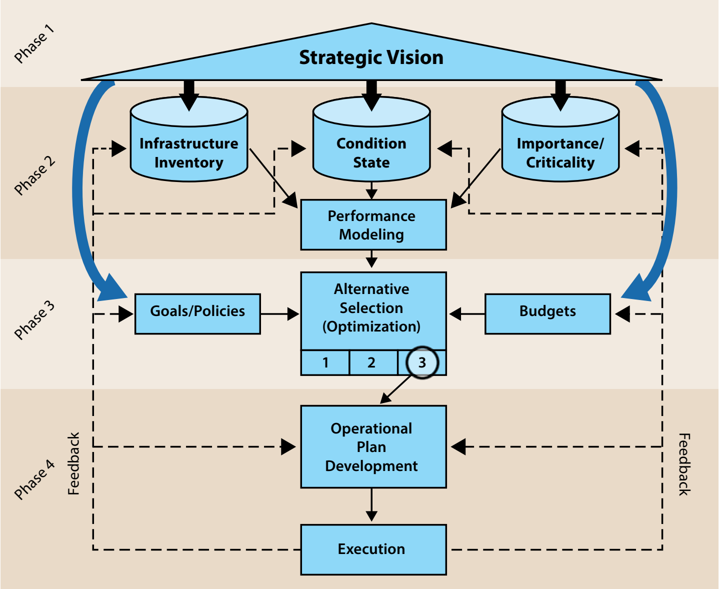
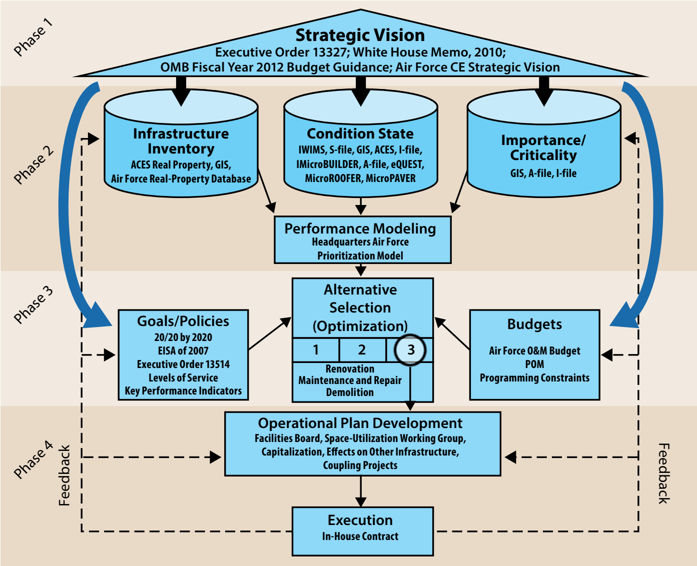


Figure 1. Logical asset-management model

The strategic components illustrated in this logical model formulate the process of asset management. Although relationships may differ according to organization, the basic artifacts of the asset-management system are considered, defined, and discussed below.

The researchers tailored this logical model specifically to the Air Force's infrastructure operations, using a representative sample of the service's infrastructure to demonstrate the model's application and validity. Figure 2 shows the general logical model (fig. 1) specifically implemented for the US Air Force. One could apply this same process to any agency with a large, varying infrastructure inventory and limited resources. In particular, figure 2 presents the Air Force case study of the logical model, which modifies the general logical model to the service's asset-management process, depicts the components as they pertain to this specific organization, incorporates Air Force entities prevalent to each component, and identifies the data needed for analysis of its infrastructure systems.



ACES – Automated Civil Engineer System
CE – Civil Engineer
EISA – Energy Independence and Security Act
GIS – Geographic Information System
IWIMS – Interim Work Information Management System
O&M – Operation and Maintenance
OMB – Office of Management and Budget
POM – Program Objective Memorandum

Figure 2. Logical asset-management model for the Air Force

The strategic asset-management components depicted in the logical model (fig. 2) comprise the process of asset management for the Air Force. To illustrate the specific Air Force application, the sections below further define and discuss each asset-management artifact.

Phase 1

Strategic vision. The strategic vision creates an umbrella under which one can align the operational aspects of data collection, budgets, policies, and goals to utilize the latest asset-management techniques.[24] Knowledge of the desired end state allows decision makers to prudently dedicate resources to the operation, maintenance, and repair of infrastructure assets.

Air Force strategic vision. National leaders and policy makers establish the overarching strategic vision. Specifically, the White House and Congress influence the strategic visions of all federal agencies, including the Department of Defense and the Air Force. The Department of Defense's strategic-level documents provide overarching guidance that the Air Force implements through its own strategic vision and operations. According to the strategic vision of the Air Force's civil engineer career field, the Office of the Air Force Civil Engineer seeks to "provide . . . efficient, sustainable installations by using transformational business practices and innovative technologies."[25] This strategic vision highlights the use of asset-management principles in daily operations and currently guides data collection, budgets, policies, and goals for the service.

Phase 2

Infrastructure inventory. By maintaining an infrastructure inventory, one can determine assets owned and their location.[26]

Air Force infrastructure inventory. The Air Force possesses an incredibly diverse set of constructed facilities and infrastructure assets, ranging from dormitories to aircraft hangars to warehouses.[27] This infrastructure, which supports a myriad of government functions, is located on numerous continents. The age of the 139,556 infrastructure assets in the Air Force's inventory spans decades—sometimes centuries—of building design and construction technologies.[28] The service collects and maintains data for its infrastructure inventory with a valid set of data-management systems in order to generate a snapshot of its assets; however, considerable information-technology issues exist because current systems do not effectively communicate with each other and data are entered numerous times into multiple data-management systems.[29] For example, the Air Force's Automated Civil Engineer System, which contains data regarding infrastructure operations such as maintenance and repair projects, hinders information flow because of its incompatibility with other MMSs, such as the Geographic Information System.

Condition state. Because infrastructure systems are in a constant state of decay, the condition state of an asset represents a snapshot of dynamic infrastructure assets.[30] Collecting condition-state data allows one to understand the current maintenance and repair necessary for infrastructure and to predict the future state of assets.[31]

Air Force condition state. The Air Force collects condition-state data in an MMS—the Interim Work Information Management System, tailored specifically for military operations. The service also utilizes MicroROOFER for the condition state of roofs and MicroPAVER for that of pavements, to name just a few. Moreover, the Air Force carries over approximately $9.3 billion of maintenance-and-repair backlog each year, which amounts to 3.5 percent of its current replacement value.[32] This quantity of deferred maintenance and repair is above the recommended industry standard of 1 to 2 percent residual from year to year.[33]

Importance and criticality. An infrastructure asset's criticality characterizes its importance or business value to an agency's operations. Agencies collect data on importance and criticality to fulfill two objectives: to understand the effect that incapacity or destruction of infrastructure assets would have on operations and to establish a relative order of significance among assets for the purpose of allocating limited resources.[34]

Air Force importance and criticality. The Air Force captures importance and criticality data to accurately assess (1) the relative significance of assets for the purpose of allocating and balancing limited resources and (2) the effect of inoperable assets on operations. The service utilizes the mission dependency index, an infrastructure metric, to link the importance and criticality of infrastructure assets to the mission of an installation. Information about importance and criticality enables decision makers to understand the link between infrastructure assets and mission accomplishment.

Performance Modeling. Performance modeling serves as the primary tool for understanding the maintenance and repair needs of infrastructure systems.[35] Decisions about maintenance and repair seek to choose the most economical (from a life-cycle standpoint) approach to determining what one should fix first.[36] In essence, such a tool relies on accurate data to guide decisions related to the established strategic vision. Thus, a dependency exists between the performance modeling tool and the strategic vision to ensure that measureable components of the tool give decision makers the necessary information to align viable approaches with the strategic vision. Ultimately, the goal is to enable them to make informed, performance-based decisions that link the goals, policies, and budget to known aspects of a system's attributes (inventory, condition state, and importance and criticality) and performance (metrics and modeling tools).

Air Force performance modeling. Performance modeling for the Air Force serves as the primary tool for prioritizing maintenance and repair requirements; toward that end, it utilizes an equation with infrastructure metrics to rank-order projects. Headquarters Air Force developed the current performance modeling tool and recently adopted an updated tool, which was implemented in 2013.

Phase 3

Goals and policies. Goals and policies arise from and align with the strategic vision to convey how an agency manages its assets; they also translate an organization's strategic vision into specific, relevant targets.[37] The latter, together with focus items, represent benchmarks that propel agencies toward realizing their desired long-term objectives. Typically, agencies define their levels of service in their goals and policies, which assist in shaping targets and constraints of the system.

Air Force goals and policies. To align with the strategic vision of providing sustainable installations by using transformational business practices, the Air Force coined the term *20/20 by 2020* to represent its goal of reducing both the physical square footage of its infrastructure as well as maintenance and repair costs by 20 percent by the year 2020.[38] The Energy Independence and Security Act of 2007, which aims to reduce energy usage by 30 percent by the year 2015; Executive Order 13514, which seeks to reduce potable water usage by 26 percent as well as nonpotable water usage by 20 percent by the year 2020; and the 20/20 by 2020 goal align with the Air Force's strategic-level vision.[39] These objectives intend to reduce the Air Force's real-property footprint to the most desirable size and incorporate energy and water conservation methods in the interest of optimizing the performance of infrastructure assets that support the war-fighting mission.[40] Ultimately, the Air Force reduces the stock of infrastructure assets as well as the maintenance and repair budget while maintaining a constant level of service and operations. This concern with the Air Force's infrastructure, which also applies to any agency with similar intiatives, reinforces the demand for a comprehensive framework to accommodate numerous infrastructure types and limited resources to inform asset-management decisions.

Budget. Budgets, which dictate the availability of resources for infrastructure projects, constitute the preeminent constraint that shapes practically every decision about asset management.

Air Force budget. Currently, the Air Force allocates $2.5 billion annually to maintenance and repair projects.[41] This budget amounts to 0.95 percent of its current replacement value, which remains significantly lower than the recommended industry standard of 2 to 4 percent.[42] Air Force regulations dictate the maximum amount available for various project types, such as $750,000 for minor construction, which imposes additional financial constraints. Allocating resources across asset types causes another budget issue for the service. Given the limited resources available, decision makers compare the worth and importance of infrastructure assets to determine which ones require resource allocation.

Alternative selection. Alternative selection explores options associated with infrastructure assets to determine which approach is in the agency's best interest. It entails examining and analyzing information from the performance modeling tool, goals, and policies as well as an understanding of financial constraints to determine the most advantageous solution. At this step in the comprehensive framework, decision makers determine the preferred resolution from the data provided.[43]

Air Force alternative selection. Under the operations and maintenance (O&M) budget, the Air Force examines four options for its infrastructure: demolish, maintain and repair, renovate, or construct an asset with capitalization.[44] The O&M budget funds demolition, maintenance and repair, and renovation projects. Capitalization, otherwise known as military construction, creates a new infrastructure asset that improves capability and corrects infrastructure issues. However, such construction falls under a separate budget with direct congressional oversight and approval; it does not compete with O&M funds.

Phase 4

Operational plan development. The purpose of operational plan development involves examining the impact of the preferred course of action on an agency's infrastructure from the perspective of second- and third-order effects. After one determines an optimal solution, operational plan development considers ways of leveraging efficiency from infrastructure networks and the effect of the proposed course of action on other aspects of these assets.[45]

Air Force operational plan development. Along with addressing how the optimal solution affects current maintenance and repair projects, planning for future endeavors (e.g., space utilization as well as future maintenance and repair projects) occurs as a part of operational plan development. The preferred course of action entails consideration for bundling projects together to gain time and cost efficiencies. One can carry out projects on connected, neighboring infrastructure systems and replace parts simultaneously—for example, completing an airfield lighting project while executing a pavement project on a runway.[46]

Execution. Preventive maintenance, reactive maintenance, project implementation, and demolition occur during execution, which involves synchronizing the previously discussed components as a means of completing projects.[47]

Air Force execution. In the case of the Air Force, execution entails coordinating the labor and funding to carry out demolition, maintenance and repair projects, and/or renovation. Execution implements the optimal solution to utilize limited resources in the most effective manner and thereby optimize the performance of infrastructure assets.

Feedback. Because asset-management frameworks are iterative, the feedback loop allows this cyclic process to reflect upon past efforts and start again.[48] The initial cycle through this comprehensive framework serves as the basis for subsequent cycles and influences future decisions.[49] Upon execution of a project, decision makers analyze the results, address any issues, and work through the framework again at the appropriate phase.

Air Force feedback. The iterative process of asset management for the Air Force requires a feedback loop. The continual movement of personnel and commanders on the headquarters staff keeps the strategic vision, goals, and policies in constant flux. Additionally, the O&M budget varies from year to year.[50] Thus, the service's decision makers examine results and address changes during feedback, prior to resuming the iterative process of asset management.

The logical asset-management model (fig. 1) establishes a comprehensive framework that offers guidance for the asset-management process. It acts as a useful decision-making tool applicable to agencies with a substantial, varied infrastructure inventory and limited resources. This framework enables decision makers to formulate viable approaches and alternatives to infrastructure management and facilitates efficient use of the annual O&M budget in order to optimize the performance of infrastructure assets.

The logical Air Force asset-management model (fig. 2) creates a decision-making framework for the service that directs the analytical process of asset management and addresses infrastructure issues specifically for this organization. This comprehensive asset-management framework confirms its general applicability to agencies with a large, varying infrastructure inventory and limited resources. It also affirms that agencies can tailor the general logical model to infrastructure systems of a particular organization, thus establishing the framework's usability and utility for agencies with similar infrastructure characteristics and budget constraints. The final step in the data-modeling process consists of developing a physical model that employs the relationships among asset-management components and their ontologies. Physical models are tailored to the specific infrastructure operations of individual agencies and their data requirements as a means of compiling information for the performance modeling tools. This article purposefully excludes the Air Force physical model that guides the implementation of next-generation information technology because it lacks applicability to other agencies with similar infrastructure characteristics and budget constraints.

Key Findings

The analysis conducted during this research effort offers two key findings that pertain not only to the Air Force but also to agencies with similar infrastructure characteristics and budget constraints. First, a discontinuity exists between the service's established strategic vision, goals, and policies and the current (equation 1) as well as recently adopted (equation 2) performance modeling tools. The logical model accentuates this disconnect, demonstrating the need for an improved tool that aligns with the Air Force's strategic vision, goals, and policies. At present, the service uses equation 1 to prioritize maintenance and repair projects:[51]

Equation 1

$$\text{Priority} = (\textit{Facility Condition Index} \text{ x } \textit{Mission Dependency Index}) +/- \textit{Commander Adjustment}$$

During alternative development, the Air Force encounters a primary limitation caused by discontinuity between the measureable metrics of its goals (the 20/20 by 2020 objective, the Energy Independence and Security Act of 2007, and Executive Order 13514) and the infrastructure metrics of the current performance modeling tool.[52] To reiterate, the 20/20 by 2020 goal wishes to reduce both the physical square footage of Air Force infrastructure as well as maintenance and repair costs by 20 percent by the year 2020; the Energy Independence and Security Act aims to decrease energy usage by 30 percent by the year 2015; and Executive Order 13514 seeks to lessen the use of potable water usage by 26 percent and nonpotable water by 20 percent by the year 2020. However, the current priority equation—equation 1 (performance modeling tool)—prioritizes projects with condition-state and infrastructure-inventory information based on each infrastructure's economic health and importance to operations (facility condition index and mission dependency index). This equation neither considers nor accounts for the objectives of 20/20 by 2020, the Energy Independence and Security Act of 2007, or Executive Order 13514 (reduction in square footage, energy usage, and water usage, respectively); it does not include energy, water, or square-footage infrastructure metrics sought by the Air Force's goals. This disconnect between the current performance modeling tool (equation 1) and goals causes decision makers to select an optimal solution based upon either the goals or the priority equation—but not both. It also produces competing interests and a lack of synergy between the goals and current performance modeling tool (equation 1). Thus, the priority order generated by the current tool does not align with established Air Force goals, creating a disconnect from the comprehensive framework and the relationships among asset-management components depicted in the framework. Additionally, decision makers will utilize the current Air Force performance modeling tool (equation 1) to prioritize maintenance and repair projects until implementation of the recently adopted performance modeling tool (equation 2) in 2013:[53]

Equation 2

$$\text{Priority} = 0.15(\textit{Health, Safety and Compliance}) + 0.10(\textit{Facility Condition Index} \times 100) + 0.15(\textit{Standardized Mission Dependency Index}) + 0.20(\textit{Local Mission Impact}) + 0.15(\textit{Cost Efficiency}) + 0.25(\textit{Service Quality})$$

The recently adopted performance modeling tool (equation 2) also accounts for the asset-management components of infrastructure inventory and condition state, as well as importance and criticality, by including the infrastructure metrics of the facility condition index, standardized mission dependency index, and local mission impact. Nevertheless, the Air Force encounters a limitation with the recently adopted performance modeling (equation 2) tool during alternative development because the latter combines goals for energy and space utilization into one infrastructure metric—cost efficiency—and does not include a water-usage metric. Although the cost-efficiency metric aligns with established goals for utilizing energy and space, it does not balance these objectives to ensure their realization. Once again, the priority order generated by the recently adopted performance modeling tool (equation 2) does not align with all of the Air Force's established goals, also generating a disconnect from the comprehensive asset-management framework and the relationships among asset-management components depicted in the framework. Thus, the Air Force needs an improved performance modeling tool that incorporates infrastructure metrics for utilizing energy, water, and space if it wishes to objectively prioritize maintenance and repair projects, compare various types of infrastructure at different locations, and produce master priority lists for its infrastructure assets.

The second key finding establishes that the data and MMS necessary for strategic-level asset management do not align with those needed for tactical-level asset management because of a lack of enterprise-wide data and an enterprise-level MMS to manage the information. The strategic level forecasts, requests, and justifies a long-term budget for demolition, renovation, capitalization, and maintenance and repair projects with a 10- to 12-year outlook. But the tactical level allocates the O&M budget and advocates for short-term requirements with a one- to two-year outlook. The tactical level (Air Force installations) funnels data—usually in an MMS—up to the strategic level, based on its own outlook. Similarly, the strategic level (Headquarters Air Force) funnels data—usually in an MMS—down to the tactical level, based on its own outlook. The top-down data transfer does not consider the tactical-level outlook, and the bottom-up data transfer does not consider the strategic-level outlook. This disparity stems from differences in operations between the two levels. Long-term planning is not a concern of the tactical level because it concentrates on short-term execution, but a lack of information regarding long-term requirements results in a dearth of requests for and justification of future budgets. Consequently, an adequate amount of O&M funds will not be available for projects in 10 years, when the long term becomes the short term. Moreover, the strategic level does not concern itself with short-term execution because it focuses on long-term planning and because funds for short-term execution have already been allocated to installations across various asset types.

Additionally, the Air Force's civil engineer community collects data for, utilizes, and maintains more than 10 MMSs. At times, the system utilized by the strategic level is not the same MMS employed by the tactical level. In these instances, the lack of compatibility between data formats hinders the top-down, bottom-up flow of information. Air Force efforts should align the data and MMS required for strategic-level asset management with those necessary for asset management at the tactical level—precisely what the comprehensive asset-management framework does. The latter streamlines communication, aligns data requirements between vertical as well as horizontal levels, and formulates resolutions in the best interest of all levels. Aligning the needed data and MMS enables transparency of information and streamlines its collection and maintenance for efficient, effective database management. The comprehensive asset-management framework for numerous infrastructure types fulfills the ultimate goal of data management—to align the MMS and necessary information for asset management so that decision makers can conceive of approaches and alternatives in the best interest of all vertical (tactical, operational, and strategic) levels of the Air Force. The discontinuity that exists between the performance modeling tools (equation 1 and equation 2) and the Air Force's strategic vision, goals, and policies—as well as the differences in MMS and data required between the strategic and tactical levels—causes misaligned data management at both horizontal and vertical levels (fig. 3).

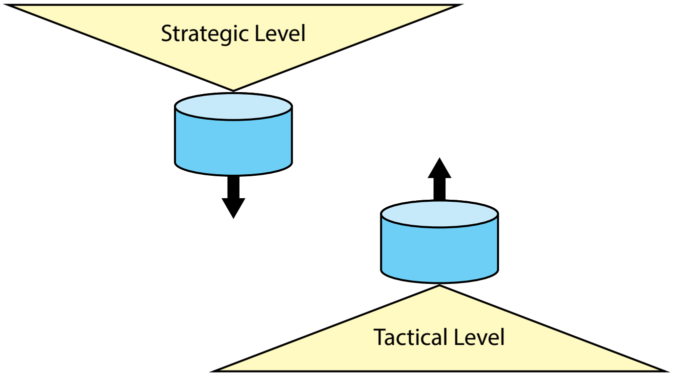


Figure 3. Data disparity between the strategic and tactical levels

Thus, creation of a single enterprise-level database for the Air Force will further the implementation of asset-management business practices. Next-generation technology would both enable implementation of the asset-management framework and provide enterprise-wide data access at all levels (strategic, operational, and tactical). A streamlined top-down, bottom-up approach with a single enterprise-level database (e.g., oracle and structured query language) and common data that aligns the strategic and tactical levels both vertically and horizontally would effectively manage and allocate resources across numerous types of infrastructure assets—the premise of next-generation technology. This approach toward integration of information technology would allow the tactical level to provide the strategic level with data applicable to its focus area and vice versa—unlike the current situation, in which the tactical and strategic levels supply the other with information that applies to their own outlook.

Conclusion

This article has identified two requirements fulfilled by developing a comprehensive asset-management framework that offers guidance for numerous infrastructure types and satisfies asset-management business principles—specifically, for agencies with a large, varying infrastructure inventory and limited resources. The utility of this research lies in its product, which contributes to asset management's body of knowledge and optimizes the performance of numerous infrastructure types at various locations. The article discussed two key findings: data disparities at both the horizontal and vertical levels as well as performance modeling tools that do not account for Air Force goals. It utilized a representative sample of Air Force infrastructure to illustrate implementation of the comprehensive asset-management framework and to demonstrate the proposed framework's utility in identifying the two key findings. Thus, agencies with constrained resources and a substantial, disparate inventory of infrastructure can conduct holistic management of infrastructure assets by applying this framework to their specific infrastructure operations. ✪

Notes

1. Michael Culver, "Transforming the CE Enterprise," *Air Force Civil Engineer Magazine* 15, no. 5 (2007): 4–12, http://www.afcec.af.mil/shared/media/document/AFD-120926-124.pdf; Department of Defense, *Operation and Maintenance Overview: Fiscal Year 2011* (Washington, DC: Department of Defense, 2010); and Maj Gen Del Eulberg, "Managing Air Force Assets," *Air Force Civil Engineer Magazine* 16, no. 1 (2008): 5–7, http://www.afcec.af.mil/shared/media/document/AFD-120926-125.pdf.

2. Culver, "Transforming the CE Enterprise," 4–12.

3. Ibid.; and United States Department of Transportation, *Economic Analysis Primer* (Washington, DC: United States Department of Transportation, August 2003), http://www.fhwa.dot.gov/infrastructure/asstmgmt/primer.pdf.

4. Joseph L. Schofer et al., "Research Agenda for Transportation Infrastructure Preservation and Renewal: Conference Report," *Journal of Infrastructure Systems* 30 (December 2010): 228–30, http://transportation.mst.edu/media/research/transportation/documents/J5_2010_Myers.pdf.

5. Culver, "Transforming the CE Enterprise," 4–12.

6. Dana J. Vanier, “Why Industry Needs Asset Management Tools,” *Journal of Computing in Civil Engineering* 15, no. 1 (2001): 35–43.

7. Dana J. Vanier, “Asset Management: ‘A’ to ‘Z,’” in *Proceedings of the American Public Works Association International Public Works Congress* (Philadelphia: American Public Works Association, 2001), 2.

8. Dana J. Vanier, “Advanced Asset Management: Tools and Techniques,” *Journal of Information Technology* 15, no. 1 (2000): 39–56.

9. Dana J. Vanier, “Asset Management 101: A Primer,” *Journal of Information Technology* 15, no. 2 (2000): 1–15.

10. C. Paul Robinson, Joan B. Woodard, and Samuel G. Varnado, “Critical Infrastructure: Interlinked and Vulnerable,” *Issues in Science and Technology*, Fall 1998, 61–67, http://www.issues.org/15.1/robins.htm.

11. Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies,” *IEEE Control Systems Magazine* 21, no. 6 (December 2001): 18–20.

12. Paul A. Longley et al., *Geographical Information Systems and Science*, 2nd ed. (West Sussex, England: Wiley & Sons, 2005), 178–79.

13. Carlo Batini, Maurizio Lenzerini, and Shamkant B. Navathe, “A Comparative Analysis of Methodologies for Database Schema Integration,” *ACM Computing Surveys* 18, no. 4 (December 1986): 333–64.

14. Longley et al., *Geographical Information Systems*, 178.

15. Thomas R. Gruber, “Toward Principles for the Design of Ontologies Used for Knowledge Sharing,” *International Journal of Human-Computer Studies* 43, no. 1 (November 1995): 907–28.

16. Longley et al., *Geographical Information Systems*, 178–79.

17. Ibid., 178; and William E. Sitzabee et al., “Data Integration of Pavement Markings: A Case in Transportation Asset Management,” *Journal of Computing in Civil Engineering* 23, no. 5 (September 2009): 288–93.

18. Longley et al., *Geographical Information Systems*, 178; and Sitzabee et al., “Data Integration of Pavement Markings,” 288–93.

19. Len Silverston, *The Data Model Resource Book*, vol. 1 (New York: Wiley & Sons, 2005), 340–42.

20. Longley et al., *Geographical Information Systems*, 178–79; and Silverston, *Data Model Resource Book*, 340–42.

21. Longley et al., *Geographical Information Systems*, 178–79; and Sitzabee et al., “Data Integration of Pavement Markings,” 288–93.

22. Longley et al., *Geographical Information Systems*, 178–79.

23. Thomas M. Connolly and Carolyn E. Begg, *Database Systems: A Practical Approach to Design, Implementation, and Management*, 3rd ed. (Harlow, England: Addison-Wesley, 2005), 52–57.

24. Australian National Audit Office, *Asset Management Handbook* (Canberra, Australia: Australian National Audit Office, 1996), 10–13.

25. Office of the Air Force Civil Engineer, *2011 U.S. Air Force Civil Engineering Strategic Plan* (Washington, DC: Office of the Air Force Civil Engineer, 2011), 8.

26. Vanier, “Asset Management: ‘A’ to ‘Z,’ ” 1–16.

27. National Research Council, *Stewardship of Federal Facilities* (Washington, DC: National Academies Press, 1998).

28. Department of Defense, *Operation and Maintenance Overview*.

29. John Thomas, “Driving CE Transformation with NexGen IT,” *Air Force Civil Engineer Magazine* 17, no. 2 (2009): 6.

30. Government Accountability Office, *Federal Real Property: Progress Made toward Addressing Problems, but Underlying Obstacles Continue to Hamper Reform* (Washington, DC: Government Accountability Office, April 2007), http://www.gao.gov/new.items/d07349.pdf.

31. Rita Ugarelli et al., “Asset Management for Urban Wastewater Pipeline Networks,” *Journal of Infrastructure Systems* 16, no. 2 (June 2010): 112–21.

32. Government Accountability Office, *Defense Infrastructure: Continued Management Attention Is Needed to Support Installation Facilities and Operations* (Washington, D.C.: Government Accountability Office, April 2008), 5, http://www.gao.gov/assets/280/274690.pdf.

33. Ibid., 2–3.

34. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2009), 102, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

35. Regina S. McElroy, “Update on National Asset Management Initiatives: Facilitating Investment Decision-Making,” in *Proceedings of the American Public Works Association International Public Works Congress* (Denver: American Public Works Association, 1999), 1–10.

36. Vanier, “Asset Management: ‘A’ to ‘Z,’ ” 1–16; Sitzabee et al., “Data Integration of Pavement Markings,” 288–93; and William E. Sitzabee, Joseph E. Hummer, and William Rasdorf, “Pavement Marking Degradation Modeling and Analysis,” *Journal of Infrastructure Systems* 15, no. 3 (September 2009): 190–99.

37. Maunsell Project Management Team, *International Infrastructure Management Manual* (New Zealand: National Asset Management Steering Group, 2006), 1.6–.8.

38. Headquarters Air Force, *Air Force Demolition Policy* (Washington, DC: Department of the Air Force, 2009); and Culver, “Transforming the CE Enterprise,” 4–12.

39. Headquarters Air Force, *Air Force Demolition Policy*; *Energy Independence and Security Act of 2007*, Public Law 110–140, 110th Cong., 1st sess., 19 December 2007, http://www.gpo.gov/fdsys/pkg/PLAW-110publ140/pdf/PLAW-110publ140.pdf; and Barack H. Obama, *Executive Order 13514—Federal Leadership in Environmental, Energy, and Economic Performance* (Washington, DC: White House, Office of the Press Secretary, 5 October 2009), http://www.whitehouse.gov/assets/documents/2009fedleader_eo_rel.pdf.

40. Maj Gen Timothy A. Byers, “20/20 by 2020 Prepares Us for Today’s, Tomorrow’s Budget Challenges,” *Air Force Civil Engineer Magazine* 18, no. 3 (2010): 3, http://www.afcec.af.mil/shared/media/document/AFD-120929-001.pdf.

41. Department of Defense, *Operation and Maintenance Overview*, 23.

42. Vanier, “Asset Management Tools,” 35–43.

43. John H. Cable and Jocelyn S. Davis, *Key Performance Indicators for Federal Facilities Portfolios* (Washington, DC: National Academies Press, 2005).

44. Department of Defense, *Identification of the Requirements to Reduce the Backlog of Maintenance and Repair of Defense Facilities* (Washington, DC: Department of Defense, 2001), 91–96.

45. R. Coullahan and C. Siegfried, “Facilities Maintenance Using Life Cycle Asset Management,” *Facilities Engineering Journal* 12, no. 1 (1996): 1–16.

46. National Research Council, *Stewardship of Federal Facilities*, 30–34.

47. Cable and Davis, *Key Performance Indicators*, 10–14.

48. National Association of College and University Business Officers, *Managing the Facilities Portfolio* (Washington, DC: National Academy Press, 1995), 12–16.

49. Maunsell Project Management Team, *International Infrastructure Management Manual*, 2.36–.38.

50. Government Accountability Office, *Federal Real Property*, 4–15.

51. Headquarters Air Force, *Activity Management Smart Book* (Washington, DC: United States Air Force, 2009), 5–6.

52. Culver, "Transforming the CE Enterprise," 4–12; Headquarters Air Force, *Air Force Demolition Policy*; *Energy Independence and Security Act of 2007*; Obama, *Executive Order 13514*; and Byers, "20/20 by 2020," 3.

53. Headquarters Air Force, *Restoration and Modernization Integrated Priority List Model* (Washington, DC: Department of the Air Force, 2011), 2.

Lt Col William E. Sitzabee, PhD, PE, USAF

Lieutenant Colonel Sitzabee (BSCE, Norwich University; MS, Air Force Institute of Technology; PhD, North Carolina State University) is the commander of Air Force ROTC Detachment 520, Cornell University, and a professor of aerospace studies. His research interests include facility and infrastructure management from an asset-management perspective. Lieutenant Colonel Sitzabee is a registered professional engineer with more than 19 years of experience in senior-level facilities and infrastructure engineering design, construction, and contract management. He has vast construction-management experience, both deployed and in garrison, including construction of aircraft parking aprons, facility construction and operations, and force beddown. He has served as the executive officer for the commander, US Air Forces Central, as well as a commander's action group action officer and political military adviser responsible for managing the commander's staff, writing speeches, and preparing senior-executive-level presentations for both domestic and foreign audiences. Since obtaining his PhD in civil engineering, Lieutenant Colonel Sitzabee has published 23 scholarly works in 11 peer-reviewed journals.

)

Capt Marie T. Harnly, USAF

Captain Harnly (BA, BS, Stanford University; MS, Air Force Institute of Technology) is the civil engineer flight commander for the 64th Expeditionary Support Squadron, Riyadh, Saudi Arabia, leading more than 80 military and civilian personnel and managing over 225 facilities. She previously served as a programmer at Joint Base Charleston, South Carolina, where she planned and programmed sustainment, maintenance, and repair as well as military construction projects for $2.7 billion in base property and capital assets. Captain Harnly has also served as mission support group executive officer and special assistant / project officer to the commander, 82nd Training Wing, Sheppard AFB, Texas.

Let us know what you think! Leave a comment!

Disclaimer

The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

http://www.airpower.au.af.mil

Who's in Charge? Commander, Air Force Forces or Air Force Commander?

Lt Col Brian W. McLean, USAF, Retired

"I've got the stick."
"I've got the conn."
"Sir, I accept command."

Sometimes different words, appropriate at different levels, all say the same thing. Let's imagine that you are now in control (of the aircraft, the ship, or the unit) and have both the authority and responsibility that go with the position. But exactly what (or whom) do you have authority over and responsibility for? What is the extent of your authority? Of your responsibility? To whom are you responsible for the consequences of your decisions and actions? A new commander must be able to answer these essential questions. On the surface, the answers might appear simple and obvious, but in practice many people have found that what they think they understand doesn't reflect the real meaning.

The Fall 1998 edition of *Airpower Journal* included Brig Gen John Barry's article "Who's in Charge? Service Administrative Control"—an excellent overview of the role and authority of an Air Force commander as we understood the position at that time. In the 15 years since the appearance of that article, Airmen have gained much better comprehension of the command of Air Force forces (AFFOR), especially with the help of publications such as Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine, Organization, and Command*; the *Air Force Forces Command and Control Enabling Concept* and its implementing program action directives; and practical experience in Operations Enduring Freedom and Iraqi Freedom.[1] As General Barry foresaw, "Command authority has once again become a serious subject of discussion . . . in light of the multiple contingency taskings our Air Force has responded to."[2] It is appropriate to revisit the issues raised by the general in light of our experiences since fall 1998.[3] Discussion of the command and control of AFFOR, especially in deployed operations, first requires a common understanding of three critical terms: *Air Force commander*; *commander, Air Force forces*; and *chain of command*.

Air Force Commander

The beginning of wisdom is calling things by their right names.

—Confucius

It is important to distinguish between an Air Force commander and a commander, Air Force forces (COMAFFOR). They are not necessarily synonymous titles. The former refers to any Air Force commander within a service context. The latter is reserved exclusively for the senior Air Force commander directly responsible to a joint force commander (JFC) within a joint context. Just as all tigers are cats, but not all cats are tigers, so is every COMAFFOR an Air Force commander, but not every Air Force commander is a COMAFFOR.

What is an Air Force commander? Interestingly, neither Air Force nor joint doctrine includes an official definition of the general term *commander*. Rather, definitions refer to a specific level of position of commander (e.g., JFC, service component commander, joint force air component commander). We find the best official description of a commander in Air Force Instruction (AFI) 38-101, *Air Force Organization*: "an officer who occupies a position of command pursuant to orders of appointment or by assumption of command according to AFI 51-604."[4] AFI 51-604, *Appointment to and Assumption of Command*, and AFI 38-101 go into the particulars regarding the various levels and types of Air Force units for which a commander may be designated, but neither provides more details about or a definition of an Air Force commander.[5] From the available description, however, we may conclude that an Air Force commander is an Air Force officer in charge of any Air Force unit or organization. All Air Force commanders are cats.

Commander, Air Force Forces

A COMAFFOR, though, is a different animal. Let's start with the basic definition: "The title of COMAFFOR is reserved exclusively to the single Air Force commander of an Air Force Service component assigned or attached to a JFC at the unified combatant command, subunified combatant command, or joint task force (JTF) level."[6] Three critical terms are embedded in this definition: *joint force*, *joint force commander*, and *service component command*.

- A joint force is one composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single JFC.[7]
- joint force commander. A general term applied to a combatant commander, subunified commander, or [JTF] commander authorized to exercise combatant command (command authority) or operational control [OPCON] over a joint force.[8]
- Service component command. A command consisting of the Service component commander and all those Service forces, such as individuals, units, detachments, organizations, and installations under that command, including the support forces that have been assigned to a combatant command or further assigned to a subordinate unified command or joint task force.[9]

According to joint doctrine, for every level of joint force that has AFFOR assigned or attached to it, there exists an Air Force service component command. Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, notes that "all joint forces include Service components, because administrative and logistic support for joint forces are provided through Service components."[10] The commander of the Air Force service component command is the COMAFFOR.

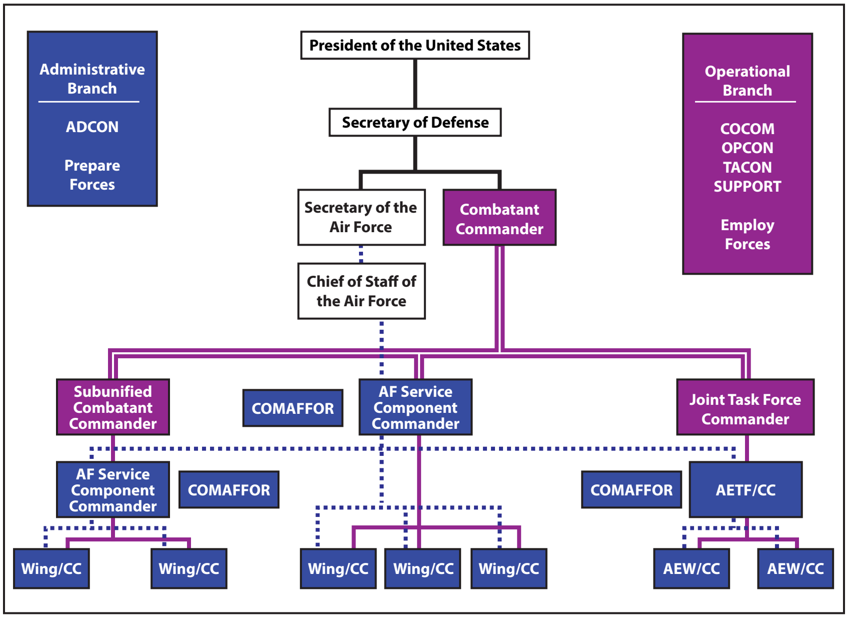
From these interrelated definitions, we can determine four key elements of a COMAFFOR:

1. The position of the COMAFFOR and its associated authorities and responsibilities apply *only* within the context of an organized joint force.
2. The COMAFFOR is the US Air Force service component commander within that joint force and presents the single Air Force voice to the JFC.
3. The JFC normally delegates OPCON (the authority to organize commands and forces and employ those forces to accomplish the assigned mission—in colloquial terms, the authority to put forces in harm's way) over all assigned or attached AFFOR within that joint force to the COMAFFOR.
4. No Air Force commander intervenes between a COMAFFOR and the JFC to whom that COMAFFOR is assigned or attached.

Chain of Command

The third point for potential confusion comes in the description of the chain of command as well as the commander's authorities and responsibilities within that chain. Even the term *chain of command* promotes uncertainty. Use of the singular noun *chain* implies that it is a single line stretching from the commander in chief to the most junior Airman in the field. But as described in joint and service doctrine, the chain of command actually includes two separate but interrelated branches—the operational and the administrative (see the figure on the next page).[11] The operational branch (in purple) runs from the president through the secretary of defense to the commanders of combatant commands and then to the Air Force service component commanders. The administrative branch (in blue) runs from the president through the secretary of defense to the service secretaries and then—to the extent determined by the service secretary or allowed by law—

through the service chiefs to the service forces. The two branches diverge at the secretary of defense and then reconverge at the Air Force service component commander, the most senior Air Force commander immediately subordinate to the JFC.



ADCON - administrative control
AETF - air and space expeditionary task force
AEW - air expeditionary wing
CC - commander
COCOM - combatant command (command authority)
COMAFFOR - commander, Air Force forces
OPCON - operational control
TACON - tactical control

Figure. Air Force forces within the chain of command. (Derived from Air Force Doctrine Document 1, *Air Force Basic Doctrine, Organization, and Command*, 14 October 2011, 89, fig. 7.1, http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd1/afdd1.pdf; and Joint Publication 1, *Doctrine for the Armed Forces of the United States*, 25 March 2013, II-10, fig. II-3; IV-3, fig. IV-1; IV-6, fig. IV-2; IV-10, fig. IV-4; IV-11, fig. IV-5, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.)

The Chain of Command for an Air Force Commander

Determining the chain of command for an Air Force commander depends upon the color of the hat worn by the next-senior commander above. If that commander wears a purple hat, then the Air Force commander responds to both a joint and an Air Force chain of command. Within the joint structure, the Air Force commander is under a combatant commander and possibly either a subunified combatant commander or a JTF commander. Furthermore, as previously discussed, an Air Force commander whose next senior commander wears a purple hat is the COMAFFOR.

The COMAFFOR commands the AFFOR, defined by the *Air Force Forces Command and Control Enabling Concept* as the "USAF component assigned to a [JFC] at the unified, subunified, or Joint [JTF] level. AFFOR includes the COMAFFOR, the AFFOR staff (A-staff/personal staff), the [air and space operations center], and all USAF forces and personnel assigned or attached."[12] Neither the program action directive nor Air Force doctrine offers further definition or modification to that of the *Enabling Concept*. Instead, Air Force doctrine relies upon the previously cited joint definition of a service component: "A command consisting of the Service component commander and all those Service forces, such as individuals, units, detachments, organizations, and installations under that command, including the support forces that have been assigned to a combatant command or further assigned to a subordinate unified command or joint task force."

Depending upon the specific joint force involved, the AFFOR may be either permanent units (numbered air force / wing / group / squadron) or expeditionary (numbered expeditionary air force / air expeditionary wing / air expeditionary group / air expeditionary squadron) or some mixture of both. Note that nothing in the Air Force or joint description of the COMAFFOR mentions aircraft. The COMAFFOR is the senior Air Force commander over all AFFOR, including the people, installations, and organizations assigned or attached to a JFC, whether or not those organizations include aircraft.

As shown in the figure, the chain of command above the COMAFFOR flows from both the separate operational and administrative branches so that, in effect, the COMAFFOR answers to two masters. Within the operational branch, the COMAFFOR is subordinate to the JFC (a purple hat). Within the administrative branch, the COMAFFOR is subordinate to the next-superior Air Force commander (a blue hat). Thus, the COMAFFOR could be in a potentially awkward position if the orders coming from his or her operational-branch JFC conflict with those from the administrative-branch Air Force commander. In that case, the administrative-branch authority is subject to the operational-branch authority, and the JFC's orders take precedence.[13]

For AFFOR below the COMAFFOR, the next-senior commander wears a blue hat, and the issue is less challenging. Since the two branches merge at the COMAFFOR, the chain of command for AFFOR below the COMAFFOR (including subordinate Air Force commanders) comes from a single point. Whether subordinate AFFOR commanders employ forces (operational branch) or prepare them for employment (administrative branch), the source of the authority for both branches comes from the COMAFFOR. In terms of a joint force, the COMAFFOR is part of that chain of command and is the senior Air Force commander within the joint force. This arrangement, which provides unity of command for AFFOR responding to orders from both the joint operational branch and the service administrative branch, is the critical link to unity of command.[14]

For AFFOR not assigned or attached to a JFC (e.g., Air Force Materiel Command and Air Education and Training Command forces or Air Combat Command forces not deployed or attached to a JFC for contingency operations), the situation is even simpler. In these circumstances, there is no purple-hat commander and no COMAFFOR—only an increasingly senior series of Air Force commanders. In these cases, the operational branch of the chain of command does not exist. The Air Force commander in these circumstances remains under the administrative branch of the chain of command only and exercises administrative control (ADCON) as delegated from his or her Air Force senior commander.

The Authorities of an Air Force Commander

Which authority does the Air Force commander need? Well, it depends upon what that commander is tasked to do. Will he or she order forces into harm's way? If so, then the commander needs operational branch authority of either OPCON or tactical control. As described in JP 1, these include

- authoritatively directing all military operations and joint training;
- organizing and employing commands and forces;
- assigning command functions to subordinates;
- establishing plans and requirements for intelligence, surveillance, and reconnaissance activities;
- suspending subordinate commanders from duty; and
- providing local direction and control of movements or maneuvers to carry out the mission.[15]

For force employment, the COMAFFOR supplies this operational branch authority for all subordinate Air Force units through the exercise of OPCON as delegated from the JFC (purple hat). Normally, the COMAFFOR will retain OPCON at his or her level. However, depending upon the operational circumstances and mission requirements, the COMAFFOR does have the authority to further delegate all or some portion of OPCON to a subordinate Air Force commander. Therefore, as the service component commander to a JFC, the COMAFFOR is responsible for employing the Air Force component in response to the JFC's orders.

But what if an Air Force commander is preparing forces in accordance with Air Force standards to go into harm's way? Even when this occurs in response to OPCON (e.g., a mission rehearsal or joint exercise prior to deployment), an Air Force commander exercises ADCON to provide properly equipped, manned, and trained AFFOR for tasked missions and functions. With this blue hat and ADCON, the COMAFFOR ensures the Air Force component's proper organization, training, equipment, and sustainment for employment. Again referring to JP 1, AFDD 1, and AFI 51-604, we see that the authorities of ADCON include

- administration and support responsibilities identified in Title 10, *United States Code*,
- organization of service forces,
- control of resources and equipment,
- personnel management,
- logistics,
- individual and unit training,
- readiness,
- mobilization and demobilization, and
- discipline.[16]

The figure above shows that the COMAFFOR, as the service component commander, also exercises service ADCON over all assigned or attached AFFOR. ADCON, the authority necessary to fulfill military department responsibilities for administration and support, runs from the president through the secretary of defense to the secretary of the Air Force. To the degree established by the latter or specified in law, this authority then runs through the chief of staff of the Air Force to the Air Force service component commanders assigned to the combatant commanders and to the commanders of forces not assigned to the combatant commanders. ADCON is not a war-fighting authority in the sense that it does not include the authority to direct military operations. However, it remains critically important to a war fighter since a commander cannot employ forces unless they have been properly prepared and sustained for the tasks they will perform.

As mentioned previously, the operational branch takes precedence over the administrative branch. For example, arranging the service organizational structure to meet operational mission requirements would normally be a responsibility of the service administrative branch carried out solely under ADCON. However, the operational branch's authority of OPCON does include the authority to "prescribe the chain of command to the commands and forces within the command."[17] Consequently, with OPCON a JFC may direct the reorganization of assigned and attached AFFOR even if doing so is not in accordance with Air Force standard practice. JP 1 also asserts, however, that such change should occur in consideration of service input: "With due consideration for unique Service organizational structures and their specific support requirements, organize subordinate commands and forces within the command as necessary to carry out missions assigned to the command."[18] Moreover, with regard to unit integrity, it notes that "component forces should remain organized as designed and in the manner accustomed through training to maximize effectiveness. However, if a JFC desires to reorganize component units, it should be done only after careful consultation and coordination with the Service component commander."[19] At this point, the position of the COMAFFOR as the point of convergence between the operational and administrative branches can become critically important. The COMAFFOR, an expert in the capabilities and limitations of AFFOR, understands the impact that reorganization of the latter will have on their ability to attain operational objectives.

We must realize, though, that ADCON is not exclusive to the COMAFFOR; for attached forces, the home-unit Air Force commander receives a share. For operations as part of an Air Force service component to a joint force, the COMAFFOR holds ADCON authorities over the AFFOR but not total ADCON. The latter includes all actions related to administration and support of service forces from initial accession to final separation for either home-station or deployed functions. As described in AFDD 1 and both the *Enabling Concept* and its implementing program action directives, those elements of ADCON necessary to prepare and sustain the AFFOR for operational employment should be specified to the COMAFFOR. The home-unit commander retains the remaining elements. For instance, the gaining COMAFFOR normally should have authority and responsibility for providing safe and secure billeting for deployed forces, but the authority to maintain personnel records and oversee family housing at the home station remains with that station's commander. The elements of ADCON specified to the deployed COMAFFOR and those retained by the home-unit Air Force commander should be spelled out not only in the service G-series orders that establish the expeditionary organization but also in the deployment orders that attach forces to that organization.[20]

So Who Is in Charge?

Returning to the original question, we can offer a simple answer: the properly designated Air Force commander is in charge of AFFOR. An Air Force commander

- is a service commander within the administrative branch of the chain of command;
- may also be a service commander within the operational branch of the chain of command when assigned or attached to a joint force;
- exercises ADCON to organize, train, equip, sustain, and discipline AFFOR to meet service standards;
- receives service support from the next-higher Air Force commander through the service ADCON chain; and
- responds to orders from the next-higher Air Force commander in the service chain.

In addition to these responsibilities and authorities as an Air Force commander, a COMAFFOR

- is the senior Air Force commander *within the operational branch of a designated joint force commander*;
- exercises *OPCON to employ forces in response to orders from the JFC* directly above him or her in the operational branch of the chain of command;

- exercises ADCON to organize, train, equip, sustain, and discipline AFFOR in accordance with Air Force standards and procedures *in order to execute the OPCON orders*;
- receives service support from the next-higher Air Force commander through the service ADCON chain; and
- responds to ADCON orders from the next-higher Air Force commander in the service chain *as long as these orders do not conflict with the OPCON orders from the operational chain*.

In the event of a conflict between the two branches, the authority of the operational branch takes priority over that of the administrative branch.

Therefore, whether you are an Air Force commander or a COMAFFOR, you remain responsible for the Airmen under your command and have the requisite authority to carry out that responsibility. You've got the stick. Have a great flight. ✪

Notes

1. See Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine, Organization, and Command*, 14 October 2011, http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd1/afdd1.pdf; and Department of the Air Force, *Air Force Forces Command and Control Enabling Concept* (change 2) (Washington, DC: Department of the Air Force, 25 May 2006). (Hereafter *AFFOR C2 EC*.)

2. Brig Gen John L. Barry, "Who's in Charge? Service Administrative Control," *Airpower Journal* 12, no. 3 (Fall 1998): 31.

3. Note that this article limits itself to the discussion and description of an Air Force commander of Air Force forces; for that reason, it does not address the role and authorities of the joint force air component commander—a joint commander.

4. Air Force Instruction (AFI) 38-101, *Air Force Organization*, 16 March 2011, 15, http://static.e-publishing.af.mil/production/1/af_a1/publication/afi38-101/afi38-101.pdf.

5. AFI 51-604, *Appointment to and Assumption of Command*, 4 April 2006, 1–2, 5–8, http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi51-604/afi51-604.pdf; and AFI 38-101, *Air Force Organization*, 19–64, 94–98.

6. AFDD 1, *Air Force Basic Doctrine*, 55.

7. Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, 25 March 2013, I-16, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

8. Ibid., GL-8.

9. Ibid., GL-11.
10. Ibid., IV-3.
11. Ibid., II-9; and AFDD 1, *Air Force Basic Doctrine*, 55.
12. *AFFOR C2 EC*, 50.
13. JP 1, *Doctrine for the Armed Forces*, II-11; and Title 10 *United States Code*, *Armed Forces*, pt. 1, chap. 6, sec. 165.
14. AFDD 1, *Air Force Basic Doctrine*, 55.
15. JP 1, *Doctrine for the Armed Forces*, V-6.
16. Ibid., V-12; AFDD 1, *Air Force Basic Doctrine*, 57–58; and AFI 51-604, *Appointment to and Assumption of Command*, 2.
17. JP 1, *Doctrine for the Armed Forces*, V-6.
18. Ibid.
19. Ibid., V-18.
20. AFDD 1, *Air Force Basic Doctrine*, 74; and *AFFOR C2 EC*, 12.

Lt Col Brian W. McLean, USAF, Retired

Mr. McLean (USAFA; MA, Old Dominion University) is a doctrine analyst for the Joint and Multinational Doctrine Directorate of the Curtis E. LeMay Center for Doctrine Development and Education, Maxwell AFB, Alabama. He is responsible for analyzing and developing the official Air Force position on the proper integration and use of the service's forces within a joint or multinational force structure and for advocating that position as the Air Force input to joint and multinational doctrine. He is a widely recognized expert on command relationships and a regular briefer to students at Air War College and to senior Air Force leaders at Capstone, Joint Force Air Component Commander, and Joint Flag Officer Warfighting courses. A master navigator and instructor weapon systems officer, Mr. McLean flew the C-141, F-4, and, on exchange duty with the US Navy, the F-14. His staff assignments included Tactical Air Command, Pacific Air Forces, US European Command, and Headquarters Air Force, with his final assignment as a member of the initial cadre for the stand-up of the Headquarters Air Force Doctrine Center. His Air War College student paper *Joint Training for Night Air Warfare* received the Air Force Historical Foundation's 1991 Colonel James Cannell Memorial Award for best paper by a Command Sponsored Research Fellow.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

Disclaimer

The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

http://www.airpower.au.af.mil

Deployed Communications in an Austere Environment

A Delphi Study

Capt Andrew Soine, USAF
MSgt James Harker, USAF
Dr. Alan R. Heminger
Col Joseph H. Scherrer, USAF

The information and communications technology (ICT) field is undergoing a period of tremendous change. The exponential growth rate of ICT capability in recent decades, which has had an undeniable effect on every aspect of our society, will likely have ramifications for military operations in austere environments.[1] The Air Force's 689th Combat Communications Wing commissioned a study to forecast the future of mobile ICT in such environments. Researchers at the Air Force Institute of Technology chose to employ the Delphi technique as the methodology for executing this task. The following scenario, based on the results of that study, demonstrates how possible changes in ICT might affect military operations. The article then discusses relevant issues that one would need to address before such possibilities become reality.

The Scenario: Sometime during the Next 10 to 20 Years in a Country Wracked by Natural Disaster and Sectarian Strife

The stealthy remotely piloted aircraft (RPA) streaked silently over the valley. If Senior Master Sergeant Riley had blinked, he would have missed it, but he was expecting the aircraft. The sergeant watched in anticipation as the pointed, narrow cylinder dropped from an opening in the bottom of the platform. The attack drone veered and accelerated towards the north, vanishing before its payload hit the ground.

With perfect precision, the cylinder (not standard ordnance but a radio frequency–satellite communications [RF-SATCOM] network link) hit its mark—the top of the tallest mountain overlooking the valley. This new device supplied cell-phone-like connectivity to each Soldier throughout the area of operations, along with back-haul connectivity to the rest of the Department of Defense's worldwide communications network. Riley had used the backup system to enter the request only 20 minutes ago, employing a series of linked drones to send a message to the larger staging area about 400 kilometers due north. His team was responsible for securing this valley and setting up the communications infrastructure in preparation for arrival of the main force, which would conduct humanitarian-relief efforts for the local population. The latter had suffered from disastrous flooding and landslides brought about by a stronger than normal monsoon season.

A light began blinking on the small device strapped to Sergeant Riley's forearm as he walked back into the tent.

"We're back up," said Airman First Class Biggs.

"Good. Where are they?"

"About 15 kilometers to the east. Everyone's vitals are within normal, no injuries. Staff Sergeant Ramirez reports that somebody tried to take a shot but turned tail when they returned the favor. They're resuming their patrol. I'll mark it." Airman Biggs hit a few buttons on his terminal. A moment later, a chorus of beeps arose from inside the tent as everyone's armband announced to its wearer the alert and subsequent map update. Fifteen kilometers way, Ramirez hit a few keystrokes on his armband. A mortar tube automatically pivoted towards the marked sector should its services be needed.

Riley sighed in relief. The scout patrol had recently reported that it had taken some harassing fire, and then as if on cue, the primary network went down. Several warlords in this part of the country weren't thrilled about their presence, so someone had remotely hacked into the network and introduced a virus that attacked friendly tactical systems. The intelligent security systems had detected the intrusion and deployed countermeasures but not before the primary intratheater link went down. Though internationally banned, those types of technologies somehow still showed up in environments such as these. Riley grinned, wondering if his adversary had his device in his pocket when it suddenly overheated and caught fire.

"Sergeant Riley, Ramirez says his helmet cam caught a glimpse of one of the attackers, but I doubt that these guys are in the system at Langley. I saw this improved 'hostile or friendly' app on the net earlier. What we've got is tied only to the known hostiles in the system, but this new one can match the pic from Ramirez with anybody in view. If somebody crosses paths with him again, like in the village market, it'll 'paint' him," offered Biggs.

"Nice. If it's got more than three out of four stars, go ahead and pull it down," replied Riley. The online toolbox was a lifesaver, literally. Troops in the field who needed a new capability for any particular situation—or who already had one but needed an upgrade—could just download it from the secure repository practically anywhere on the planet. They could even rate it as a good app or a dud. Riley looked back at Airman Biggs and tried to remember being so young. Biggs really knew his way around this technology stuff, as was usually the case with the younger troops. Obviously a generational thing, they all grew up just expecting it to be there and ready to use. He probably wouldn't even recognize the Air Force that Riley knew when he was that age: hauling around all that comm equipment that usually did only one thing and oftentimes not all that well; bulky, fuel-hungry generators that advertised your exact location to every jerk with an AK-47 within 100 kilometers; the mountains of batteries that you had to bring in and carry around. . . .

A voice emanating from his armband brought him back to the present. "Sergeant Riley, what's your status?" It was Major Hanson. Located at the staging area, he was conducting final preparations for deployment of the main force.

"Sir, we've had a few hiccups, but nothing serious. We're on schedule, and the equipment is almost ready," Riley responded.

"Brilliant. We're bringing a few extra teams for security. Will that be an issue?"

"Shouldn't be, but it might be a good idea to throw on a couple of extra gateways to increase our bandwidth, just in case." You can never have too much bandwidth, even out here. "A few extra teams" had a wide interpretation; too many heads might start dragging down the local network. Having some cushion ready to go would be nice. Maybe he should ask for another solar power supply as well—after all, they don't take up much room.

While Riley updated the major, the network autonomously uploaded a profile of the attack to the main system at Langley. There, it would analyze the data and push out a patch with updated security algorithms. The entire theater would have immunity within the hour.

Behind the Scenario

This story sounds like something out of science fiction. However, according to the Delphi panel that offered input for this research, the technologies it describes may be in place within the next 10 to 20 years—in some cases, perhaps even sooner. A research methodology, the Delphi technique forecasts future possibilities based on expert knowledge of areas relevant to the study.[2] This method "has become a fundamental tool for those in the area of technological forecasting."[3] In fact, many researchers advocate it for research involving subjects for which a previous datum is unavailable or nonexistent.[4] R. C. Oliver and his colleagues also confirm that "Delphi is best suited for evaluating the alternatives of some definable although not necessarily narrow issue . . . in which the experience of experts is of particular value."[5] Finally, Somnath Mishra, S. G. Deshmukh, and Prem Vrat's analysis to match forecasting techniques with specific technologies found the Delphi method a particularly good fit for studies related to information technology.[6]

The National Defense University has presented four major categories of the ICT industry: hardware, software, information services, and communications. It further divides these categories into sectors such as cable, telecommunications, manufacturing, cellular phones, software, computer and networking hardware, the Internet, data storage, and associated services and applications.[7] In the context of its report, the university developed these categories to capture the state of the ICT industry as it presently exists. However, research for this article attempted to address the predicted capabilities of ICT in future states. Certain knowledge areas that would prove useful in generating a forecast—such as trends, revolutionary concepts, and both basic and applied inquiry—did not seem well represented in the existing categories as defined. Therefore, researchers at the Air Force Institute of Technology first examined major categories of the ICT field and derived five general knowledge areas more practical for forecasting future capabilities: concept design and demand, research and intellectual aspects, technology development, application, and, ultimately, employment.

No firm agreement exists on the number of panelists necessary for an effective Delphi.[8] On the one hand, Albert P. C. Chan and his colleagues find 10 members an adequate number of panelists to represent a sufficiently wide distribution of opinion.[9] On the other hand, some studies show no consistent relationship between panel size and effectiveness.[10] Regarding the minimum number of panelists, Jacques Etienne Des Marchais indicates a minimum of six.[11] Further, David Boje and J. Keith Murnighan found no effect for group sizes of three, seven, and 11.[12]

Using the Internet, academic journals, and social networking, the research team developed a list of 100 potential panelists across the five knowledge areas from organizations including academe, non–Air Force governmental organizations, and the private sector. These individuals represented a wide spectrum of involvement within the ICT industry, including concept development, research and development, technology development, application, and the employment of technology. After prioritizing the list with the sponsoring agency, the research team contacted the 25 most desirable candidates, securing the participation of eight experts.

Critics of Delphi cite the difficulty of defining those criteria that make someone an expert. For the purposes of this article, we use V. W. Mitchell's definition of an expert as one who has had a significant amount of involvement within the industry, both past and present.[13] Many studies recommend a minimum of five years of specific experience in the particular industry, which we used as the defining factor of expertise within the ICT industry.[14] All participants have between 20 and 40 years of experience in their field.

Participants on the Delphi panel included a board member of the Association of Professional Futurists who has coauthored books on the future of technology; a program manager in the area of defense electronics, communications, and signal processing; an associate professor of systems engineering specializing in information operations, mission assurance, computer and network security, quantum cryptography and information, and mission-impact assessment; a director of business development and sales for a major satellite communications group, specializing in deployable communications; a practice leader specializing in telecommunications, innovation science, and operations management who has worked at major research facilities; a chief software architect and development lead at a technology consulting group; a disaster-communications engineer at a major networking corporation; and a federal government professional in emergency response to information-technology disasters.

Although the scenario is based on the forecast developed by the Delphi panel, the latter did not create it. Rather, the authors developed the scenario to illustrate how the ideas presented in the forecast could affect the use of deployed communications in the near future. The following discussion explores issues included in the scenario that highlight changes we may expect to see in such communications during the coming years.

Bandwidth

The RF-SATCOM network link dropped from the RPA signifies one of the trends among the panelists' forecasts. As ICT evolves, despite evolutions in protocols and data-compression techniques, bandwidth requirements will continue to grow—possibly at an exponential rate. The panelists suggested that the increase in bandwidth needs stems from expanded data exchange among robots, sensors, RPAs, and personal ICT devices such as smartphones and tablets. Therefore, as we move into future engagements, the availability of usable bandwidth providing gateways to access the Global Information Grid (GIG) will escalate dramatically. The ability simply to "deploy" a unit similar to the RF-SATCOM network link in an unforgiving environment as a means of facilitating near-instant accessibility to data exchange will likely increase virtually all aspects of the campaign it supports, whether a humanitarian-relief effort in Haiti or terrorist suppression in Africa.

Satellites versus Alternatives

The experts had divergent views on how deployed communications systems would link back to the GIG. The scenario uses both projected technologies. First, the self-configuring RF-SATCOM network link acts as a gateway to the GIG, providing wireless RF connectivity to authorized devices within the area of operations. As described by the panelists, some austere locations create great difficulties for a direct satellite link. For instance, locations under high foliage, such as a jungle environment, as well as those inside hardened shelters and under water render satellites less effective. Other panelists envisioned highly mobile data links in the form of RPA relay systems. In the scenario, Sergeant Riley uses this as a temporary communications medium to request the more robust satellite-link back-haul system.

Personal Information and Communications Technology

As devices and applications converge into smaller, faster, and cheaper individual computing devices, their interfaces will evolve. The interaction will become more fluid as the interfacing experience begins to transform to sensory inputs, biological queues, and eventually human-enhancement implants. Sergeant Ramirez communicates with Airman Biggs with a device similar to current smartphones, but it also monitors his vitals via a few nonintrusive biological sensors capable of immediately alerting both the wearer and nearby allied forces if any readings fall outside a predetermined threshold. Additionally, thanks to the fact that the RF-SATCOM network link offers local device-to-device communications, the dissemination of mission-critical information and supporting data now takes place in real time—as occurred when Airman Biggs sent an alert and map update throughout the unit. This update warns friendly forces about hostiles nearby and allows Sergeant Ramirez to coordinate retaliatory fire from isolated locations, enhancing both his unit's safety and combat effectiveness. The sergeant captures and processes photos, using them to query and update the remote database. This ability signifies two possibilities. First, it underscores the necessity of global connectivity to send data to troops in rugged locations. Second, it illustrates possible advantages of an application repository providing real-time access and updates to mission-support software. According to the panelists, multiple commercial entities have already successfully implemented similar corporate repositories.

Power

The panelists also considered the powering of ICT devices, identifying power generation, storage, and distribution as areas of concern. In the scenario, Sergeant Riley reminisces about deployed forces relying exclusively on petroleum-based power generation and replaceable batteries. The panelists forecast that power generation will slowly change from current methods to technologies such as fuel cells and locally developed power that uses renewable methods such as wind, water, and sunlight. Such renewability is beneficial from more than simply an environmental standpoint. Currently, the power needed to run a forward operating base demands many fuel generators, which leave a large footprint. Additionally, the fact that generators require fuel and maintenance adds to the logistics burden. Local renewable energy sources would drastically reduce the number of support personnel and demands for supply. Power storage and distribution converged in this scenario when the sergeant thought to request another solar power supply. Panelists suggested that the incremental battery improvements, combined with personal ICT evolution that lowers power consumption, will extend ICT battery life substantially. Members of the panel suggested wireless power distribution but acknowledged that it might not be feasible in the near-to-moderate future due to radio interference and health-related risks.

Security

The panelists forecast that as our networks become more modular and based on Internet protocol, devices would become more autonomous—witness the part of the scenario when the network pushes the attack profile to Langley for automated analysis and creation of a security patch. However, some panelists cautioned that because these modular network devices may be engineered, manufactured, and programmed for autonomy outside the Department of Defense, one must consider possible security risks akin to "backdoor computing" (bypassing normal authentication and thus securing illegal remote access to a computer). The panelists concurred that data security will be a concern in the distant future. As ICT evolves, so will malicious attackers; furthermore, as personal ICT proliferates, becoming less expensive and more ubiquitous, the pool of potential attackers will grow in step with it.

The Way Ahead

It seems naïve to assume that humankind will continue to conduct traditional warfare even as ICT developments prompt new operational capabilities and demands. Instead, we should attempt to envision how the latter will improve operations. Commentary from the eight experienced ICT industry experts yielded the common trends identified and discussed above. Bandwidth requirements will increase rapidly, and back-haul systems linking forward operating locations to the GIG will develop. Satellite capabilities will multiply, just as alternatives and RPA-relayed mediums will emerge. Personal ICT devices will progress and proliferate. The convergence of applications and data services on these devices will decrease the number of tasks that they cannot perform. As power techniques develop, a "charged" device will operate substantially longer before depleting its power source. In terms of security, human nature creates a continuous, reciprocal battle of measure/countermeasure/countercountermeasure, and so forth. An interesting perspective to consider is that the forecasts we used to produce this scenario did not specify particular developments or actual capabilities; rather, they identified distinct trends and likely paths of ICT evolution. Through this perspective we can apply these trends not as a specified plan of action but as a planning tool designed to gain and maintain adversarial advantages. As President Dwight D. Eisenhower declared, "Plans are nothing; planning is everything." ✪

Notes

[1] Richard E. Albright, "What Can Past Technology Forecasts Tell Us About the Future?," *Technological Forecasting and Social Change* 69, no. 5 (June 2002): 455; Heebyung Koh and Christopher L. Magee, "A Functional Approach for Studying Technological Progress: Application to Information Technology," *Technological Forecasting and Social Change* 73, no. 9 (November 2006): 1071; Christopher L. Magee and Tessaleno C. Devezas, "How Many Singularities Are Near and How Will They Disrupt Human History?," *Technological Forecasting and Social Change* 78, no. 8 (October 2011): 1368; Luiz C. M. Miranda and Carlos A. S. Lima, "Trends and Cycles of the Internet Evolution and Worldwide Impacts," *Technological Forecast-*

ing and Social Change 79, no. 4 (May 2012): 744–65; and Béla Nagy et al., "Superexponential Long-Term Trends in Information Technology," *Technological Forecasting and Social Change* 78, no. 8 (October 2011): 1356–64.

[2] Norman Dalkey and Olaf Helmer, *An Experimental Application of the Delphi Method to the Use of Experts*, Memorandum RM-727/1-Abridged (Santa Monica, CA: RAND Corporation, July 1962), http://www.rand.org/content/dam/rand/pubs/research_memoranda/2009/RM727.1.pdf; and Norman C. Dalkey, *The Delphi Method: An Experimental Study of Group Opinion*, RM-5888-PR (Santa Monica, CA: RAND Corporation, June 1969), http://www.rand.org/content/dam/rand/pubs/research_memoranda/2005/RM5888.pdf.

[3] Harold A. Linstone and Murray Turoff, "Introduction," in *The Delphi Method: Techniques and Applications*, ed. Harold A. Linstone and Murray Turoff (Reading, MA: Addison-Wesley Publishing, Advanced Book Program, 1975), 11, http://is.njit.edu/pubs/delphibook/delphibook.pdf.

[4] Gene Rowe and George Wright, "The Delphi Technique as a Forecasting Tool: Issues and Analysis," *International Journal of Forecasting* 15, no. 4 (October 1999): 353–75, http://www.forecastingprinciples.com/files/delphi%20technique%20Rowe%20Wright.pdf.

[5] R. C. Oliver et al., *Survey of Long-Term Technology Forecasting Methodologies* (Alexandria, VA: Institute for Defense Analyses, November 2002), ES-2, http://www.dtic.mil/dtic/tr/fulltext/u2/a410179.pdf.

[6] Somnath Mishra, S. G. Deshmukh, and Prem Vrat, "Matching of Technological Forecasting Technique to a Technology," *Technological Forecasting and Social Change* 69, no. 1 (January 2002): 20.

[7] Industrial College of the Armed Forces, *Final Report: Information and Communications Technology Industry* (Washington, DC: Industrial College of the Armed Forces, National Defense University, Spring 2007), 4, http://www.nationaldefensemagazine.org/archive/2008/August/Documents/ICAFAug.pdf.

[8] Patricia L. Williams and Christine Webb, "The Delphi Technique: A Methodological Discussion," *Journal of Advanced Nursing* 19, no. 1 (January 1994): 180–86.

[9] Albert P. C. Chan et al., "Application of Delphi Method in Selection of Procurement Systems for Construction Projects," *Construction Management and Economics* 19, no. 7 (January 2001): 699–718.

[10] Fergus Bolger and George Wright, "Assessing the Quality of Expert Judgment: Issues and Analysis," *Decision Support Systems* 11, no. 1 (January 1994): 1–24; and Klaus Brockhoff, "The Performance of Forecasting Groups in Computer Dialogue and Face-to-Face Discussion," in Linstone and Turoff, *Delphi Method*, 285–311.

[11] Jacques Etienne Des Marchais, "A Delphi Technique to Identify and Evaluate Criteria for Construction of PBL Problems," *Medical Education* 33, no. 7 (July 1999): 505.

[12] David M. Boje and J. Keith Murnighan, "Group Confidence Pressures in Iterative Decisions," *Management Science* 28, no. 10 (October 1982): 1195.

[13] V. W. Mitchell, "The Delphi Technique: An Exposition and Application," *Technology Analysis and Strategic Management* 3, no. 4 (1991): 340.

[14] Ibid., 356; and Rowe and Wright, "Delphi Technique as a Forecasting Tool," 371.

Capt Andrew Soine, USAF

Captain Soine (BS, Louisiana Tech University; MS, Air Force Institute of Technology) is a program manager with the Manufacturing and Industrial Technologies Division, Materials and Manufacturing Directorate, Air Force Research Laboratory, Wright-Patterson AFB, Ohio. He is responsible for planning, managing, and executing programs that provide advanced manufacturing processes, techniques, and technologies for timely, high-quality, and economical production and sustainment to strengthen the defense industrial base under the Title III program of the Office of the Secretary of Defense's Defense Production Act. He also addresses Air Force systems through the service's ManTech program. Captain Soine previously served in the Space Development and Test Directorate, Kirtland AFB, New Mexico; the 580th Aircraft Sustainment Group, Warner-Robins Air Logistics Center, Georgia; and as air and ground movement officer in charge with the US Army Corps of Engineers, Afghanistan Engineer District, Kabul, Afghanistan.

MSgt James Harker, USAF

Master Sergeant Harker (BS, New York Institute of Technology; MS, Air Force Institute of Technology) is the wing deployment manager for the 689th Combat Communications Wing, Robins AFB, Georgia. He is responsible for ensuring the combat readiness of equipment valued at $460 million and 1,500 Airmen from 10 squadrons composing two groups. Master Sergeant Harker has managed several work centers charged with various functions, including the maintenance of security systems that guard nuclear assets and the dissemination of Armed Forces Network radio and television broadcasts to their intended audiences. He also completed a special-duty assignment as an academy military trainer at the United States Air Force Academy, where he introduced cadets to the enlisted perspective and facilitated their development as future leaders.

Dr. Alan R. Heminger

Dr. Heminger (BA, University of Michigan; MS, California State University–East Bay; PhD, University of Arizona) is an associate professor of management information systems at the Air Force Institute of Technology, Department of Systems Engineering and Management. He has a background in networked collaborative work systems, strategic information management, and business process improvement. Dr. Heminger has undertaken research and consulting for Air Force and Department of Defense agencies, including Air Force Materiel Command, the Air Force Research Laboratory, the Air Force Center for Systems Engineering, Air Force Special Operations Command, the Air Force Office of the Chief Information Officer, the Air Force Communications and Information Center, the Defense Threat Reduction Agency, the 689th Combat Communications Wing, and the Defense Ammunition Center.

Col Joseph H. Scherrer, USAF

Colonel Scherrer (BSEE, Washington University in Saint Louis; MBA, Boston University; MS, Air Force Institute of Technology; MA, Naval War College; MA, Air War College) is commander of the 689th Combat Communications Wing, Robins AFB, Georgia. He leads 1,500 duty Airmen in an expeditionary cyber operations mission that deploys combat communications and air traffic control as well as landing-systems capabilities in permissive and nonpermissive contingency environments. A distinguished graduate of the Air Force Reserve Officer Training Corps program, Air Force Institute of Technology, Advanced Communications Officer Training School, Naval War College, and Air War College, Colonel Scherrer is the coauthor (with Lt Col William C. Grund) of *A Cyberspace Command and Control Model* (Maxwell Paper no. 47, 2009). He has participated in several theater operations, including Deny Flight, Provide Promise, Joint Forge, Deliberate Force, Southern Watch, and Enduring Freedom. He has commanded a cyber wing, a mission support group, and three communications squadrons. Colonel Scherrer has served in a variety of engineering, fixed communications, tactical communications, and staff assignments, including the Joint Staff, where he authored the Department of Defense's first national military strategy for cyberspace operations.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

Disclaimer

The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

http://www.airpower.au.af.mil

Missile-Warning Augmentation

A Low-Risk Approach

Jeffrey K. Harris
Gilbert Siegert

Recent operational successes with new space-based capabilities offer important reminders of our dedication to a strong space program for national security. Our military and intelligence operational responsibilities worldwide demand timely intelligence, surveillance, reconnaissance, warning, and communications to maximize the effectiveness and efficiency of the force. Investments in research, development, production, and operations have yielded important space-based mission capabilities that differentiate the United States and its allies in the execution of national security objectives.

The dependence of US national security on space continues to grow. A drumbeat of studies, reviews, speeches, articles, and congressional testimony, however, carries a clear message: (1) US national security space systems cost too much and take too long to go from concept refinement to deployment; (2) threats to our space capabilities are significant and increasing—if left unaddressed, our space infrastructure will become more vulnerable, fragile, and indefensible; and (3) the current US financial situation, including potentially draconian defense cuts, challenges the continuation of status quo acquisitions.

This article seeks to realistically address documented risks associated with a rapid transition from baseline space-program architectures if that transition involves immature technology alternatives. It draws on past Government Accountability Office (GAO) reports, studies, and program histories to raise awareness of the significant threats to successful operations and program acquisition when architectural transition decisions rely on unproven design and limited understanding of the ability and cost of production. The article includes direct reference to overhead persistent infrared (OPIR) architectural-transition concepts currently under consideration with the advent of disaggregation approaches by the Space and Missile Center. Initial concepts introduced by the center include changing from the space-based infrared system (SBIRS) to a wide field of view (WFOV) disaggregated approach.[1] This article recommends a judicious, low-risk demonstration and prototyping approach to insert capability, retire risk, and realize enhanced estimation of production and manufacturing costs.

Reinventing Space

Recently, Air Force leaders have made efforts to explore new architectures and acquisition strategies as potential solutions to the perceived high cost of continuing legacy space programs. Today most of the service's constellations consist of a few large, highly capable (typically multimission) spacecraft. Specifically, these new candidate architectures advocate the distribution of mission capabilities onto a variety of platforms—commercial or smaller, purpose-built craft. This concept, termed *disaggregation*, urges the United States to "buy capabilities in smaller capacity increments, distributed across more but smaller satellites or hosted payloads, and migrate ground segments to (shared), modular, open architectures."[2] Interestingly, OPIR already represents a disaggregated architecture that uses multiple, different orbits; free-flying and hosted payloads; and a distributed ground architecture to support a number of mission users. Is the national security community ready to begin such an extensive and, some would say, radical transition to additional new architectural- and capability-procurement approaches—especially when one considers that our current systems are just beginning to demonstrate significantly enhanced performance and functionality beyond expectation?[3]

Although the OPIR mission area has existed for decades as overhead nonimaging infrared with SBIRS and other systems, it is now the new kid on the block, integrating target-signature nuances, time, and place into persistent intelligence and operational products that bring exciting capabilities to the war fighter. The timely, near-seamless integration of observations provides discriminating capabilities. Users, now responding with analytic tools and techniques to best exploit the new capabilities, are only beginning to understand how to utilize the amazing new data. Having recently tested the downloading of OPIR sensor data directly to handheld devices to enhance battlespace awareness, the Army wants to pursue additional experimentation under the proposed Joint Capability Technology Demonstration.[4] Furthermore, the SBIRS Program Office is pursuing use of SBIRS infrared data to support requirements for weather and climate information.[5]

Expanding Overhead Persistent Infrared's Sensor Capabilities

The Alternative Infrared Satellite System (AIRSS), a new program started in the Department of Defense's (DOD) budget for fiscal year 2007, was intended to substitute for the geosynchronous Earth orbit (GEO) satellite segment of the SBIRS High program and produce a replacement for the US Defense Support Program's (DSP) missile-warning satellites.[6] According to a GAO report of 2007, the DOD was not pursuing the AIRSS as a "plan B" program as originally envisioned. Rather than seek to maintain continuity of operations, the program focused on advancing capabilities. Moreover, it did so within highly compressed time frames. DOD stakeholders disagreed regarding the wisdom of this approach, given past experiences with space acquisitions.[7]

The current Commercially Hosted Infrared Payload (CHIRP) experiment derives from the AIRSS program, also known as third-generation infrared surveillance legacy. Upon termination of the latter, the Operationally Responsive Space Office and SBIRS Program Office continued work on the hosted flight demonstration to advance process development of hosted payloads and conduct on-orbit testing of the CHIRP focal plane array at the least cost. Science Applications International Corporation's WFOV sensor is integrated on the SES-2 commercial geosynchronous communications satellite built by Orbital Sciences Corporation to validate missile-warning technologies from GEO in a fast and cost-effective manner. The CHIRP sensor features a fixed telescope that can view one-quarter of the earth from GEO. The infrared sensor will test the potential of its WFOV capabilities for future OPIR missions for the Air Force.

The ongoing WFOV demonstration encompassed by the CHIRP experiment helps to retire risk associated with incorporation of WFOV technology into missile-warning architectures and informs us of issues in the commercial hosting of payloads. However, it represents only a first step toward addressing the many performance, architectural, and manufacturing feasibility risks identified in numerous acquisition reviews. Transitioning from the SBIRS architecture that must meet demands across a number of mission areas—missile warning, missile defense, battlespace awareness, and technical intelligence—to a new, disaggregated architecture that will rely principally on WFOV technology carries significant mission risk at this time.

The CHIRP WFOV missile-warning (evaluation) sensor leveraged limited new-sensor focal-plane-array chip-production capabilities derived from the AIRSS program. A recently completed Burdeshaw Associates study of sensor performance notes that

> these WFOV designs contemplate use of large format staring arrays to provide full earth disk coverage in a series of optical payloads without dynamically adjusting the optical path. The stated, but unproven, advantage to the WFOV design paradigm is in reducing complexity, and therefore cost, through:
>
> - Elimination of an optical path element such as the mirror assembly
> - Elimination of moving mechanisms
> - Elimination of ground tasking software for the moving mechanisms
> - Use of commonly available optics for low(er) cost telescopes.[8]

The expanding missions in OPIR demonstrate the need for precise geolocation performance. Since the performance necessary to meet mission requirements depends upon position knowledge of all payloads so they operate as one, the latter drives integration precision, spacecraft stability, ephemeris, and line-of-sight knowledge. As a consequence of this complexity, these design parameters must also accommodate overlapping of the coverage of independent sensor payloads in order to interleave pixels to meet mission demands for geospatial resolution. Plans for the CHIRP experiment did not include validation for this criterion. The fundamental technology upon which WFOV uniquely depends—large-format, high-pixel-count infrared focal planes with thousands of pixels per side—is still maturing in uniformity and defect rates relative to the stringent target-detection needs of missile warning and the other OPIR missions.

Current WFOV sensor alternatives are under consideration as a payload that can be either hosted by or deployed on a small satellite. The coverage capability expands by integrating a focal plane array that contains 3,000 by 3,000 detectors (3K x 3K focal plane array) in combination with various optics options from four degrees to 14 degrees. By using such options, the focal plane array can observe greater geographic areas. However, the expanded coverage areas result in less geospatial resolution because as coverage increases, resolution suffers, adversely affecting the ability to discriminate individual launches from closely spaced launch locations until sufficient separation of the trajectory occurs. The strategic and theater components of the OPIR missile-warning requirements assess raid-counting accuracy and complete understanding of the boost-phase track as an imperative to quickly warn of and characterize an inbound attack to support responsive decision making. These design trades are important in determining system performance. The Burdeshaw Associates study reveals that

- WFOV is desirable technology, but the remaining design and production challenges preclude near term proven technology availability. The present sensitivity provided by these designs may be insufficient for current upper stage threats and many emerging threats.
- Affordable uniformity and defect rates in large medium wave infrared (MWIR) formats is still a work in progress.
- The wide field coverage combined with available large format focal planes limits the aperture size to those much smaller than SBIRS.

> Simply stated, sensitivity requires photons, and the number of photons is a function of aperture size.
>
> - Separation and counting of targets in realistic scenarios is poor and a real concern.
>
> To help improve target discrimination, the WFOV designs have added a moving filter wheel to the optical path to accommodate additional infrared spectral bands. This increases complexity and cost over a CHIRP-like staring array.[9]

Some realities of WFOV payload integration with host vehicles may call for additional technology and engineering. The Burdeshaw Associates study draws from a survey of industrial-base analyses which conclude that

> - WFOV may need to add image motion compensation mirrors in the optical path to retain image quality due to spacecraft bus vibrations, stability and drift characteristics that would otherwise spoil the optical image and its registration necessary for the success of imaging processing techniques and geolocation.
> - The relatively slender WFOV multi-telescope designs will need a sufficiently stiff integrating structure to transfer attitude reference from telescope to telescope to maintain micro-radian level absolute bore-sight knowledge potentially precluding lower cost commodity bus options.
> - An internal self contained line of sight knowledge calibration capability will be an essential part of WFOV payload design maturity.
> - A thermal, solar and sun outage protection design must be completed to mature WFOV payload design. This is a special challenge for hosted WFOV payloads where CONOPS [concept of operations] flexibility may be restricted by primary commercial mission priority.[10]

The WFOV designs must address these complexities early in the acquisition to assure a smooth, predictable transition to the new technology.

Staff assessments by the Office of the Secretary of Defense conclude that required functional availability precludes transition from SBIRS prior to procurement of SBIRS spacecraft GEO 6 due to the alternative development timelines. Thus, meeting the need date for SBIRS GEO 7—assuming a new start in fiscal year 2014—involves risk. In today's fiscal climate, the Office of the Secretary of Defense is struggling with simultaneously pursuing a new architecture while completing/sustaining its current missile-warning architecture. Unlike the decision during the 1990s to transition from the DSP—the previous OPIR spacecraft used for missile-warning detection—to SBIRS, no stored DSP or SBIRS spacecraft are available to reduce operational hazards should acquisition delays, performance failures, or launch disasters delay successful new architectural deployments. Comparing the present situation with the one in 1994 is revealing:

- In 1994 the missile-warning architecture was very robust with more than 20 years of sustained DSP operations, spares on orbit, and six more satellites (DSP 18–23) in production, resulting in low operational risk and time to design and develop SBIRS.
- Presently the missile-warning architecture reflects declining health of remaining DSP satellites, a single SBIRS GEO 1 spacecraft on orbit, and SBIRS GEO 2–4 in production, reflecting far less architectural robustness.

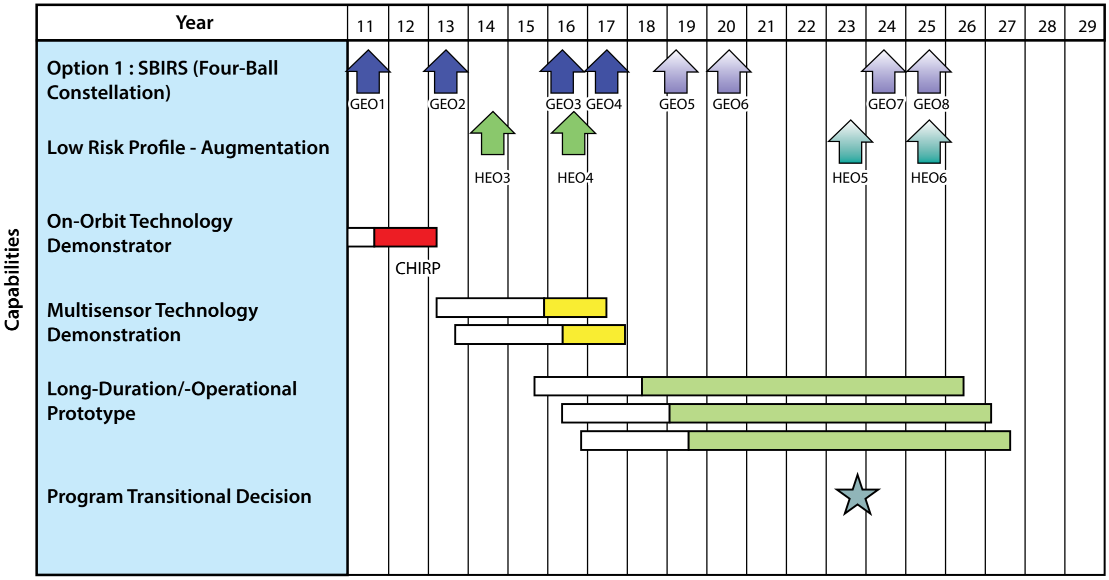
Moreover, acquisition history has repeatedly demonstrated that cost assessments of revolutionary alternative architectures are generally quite optimistic due to frequent underestimation of systems engineering, program management, nonrecurring engineering, operational integration, and launch operations. The cost of ground infrastructure is often assumed neutral among alternatives. In this case, however, disaggregated architectures requiring large numbers of sensor hosts will surface new and possibly unexpected problems in management, infrastructure, and data integration.

Possible Profile of a Low-Risk Augmentation Program

Over the last several decades, we have learned many painful lessons concerning space system development (SBIRS, the Transformational Communications Satellite, space-based radar, etc.), probably the most significant of which concerns the critical nature of mature technology. Transitioning new technologies into comprehensive acquisition programs favors diligent early efforts to demonstrate the performance of those technologies and to evolve toward a full prototype prior to commitment to full production programs. This circumstance appears very relevant to OPIR WFOV alternatives.

Consequently, we need a structured approach that reduces the likelihood of both performance problems and schedule delays through judicious, step-by-step demonstration of individual spacecraft development, production, and performance as well as multispacecraft architectural performance and impact. Key elements of that approach should include (1) sustaining the operational mission of foundational capability throughout transition, (2) fully assessing the operational performance of new technology during transition from demonstrator to prototype, (3) validating final operational performance and production costs during prototype development, and (4) understanding architectural implications.

Figure 1 depicts a structured serial approach that minimizes costs through the transition while retiring performance, production, and manufacturing pitfalls. The Burdeshaw Associates study offers an example of the schedule and elements associated with a low-risk maturation program leading to an architectural alternative and/or follow-on. The dark blue and green arrows reflect SBIRS spacecraft already in production; the light blue arrows reflect those spacecraft that need additional funding and the estimated dates for delivery to mitigate operational degradation to the mission. The figure shows the three phases of the alternative augmentation technology program, indicating development and production as clear boxes and on-orbit evaluation timelines as red, yellow, and green boxes. The star represents the study's first estimate of a decision point for moving to a new missile-warning architecture.



GEO - Geosynchronous Earth Orbit
HEO - Highly Elliptical Earth Orbit

Figure 1. Profile of a low-risk augmentation program

Sustain Operational Mission throughout Transition

Fortunately, SBIRS performance is exceeding expectations. We understand its costs and risks of production; further, with the procurement of SBIRS GEO 7 and 8 and highly elliptical Earth orbit (HEO) 5 and 6, we can expect that sustained capability will support all four mission areas through 2030. This offers the DOD a sustained period during which it can thoroughly evaluate and develop WFOV capabilities and follow a minimal annual investment approach to reduce midterm and long-term risk. By maturing the mission requirements of the WFOV constellation, technical capability, and architectural approach, the department can reach a transition point based upon comprehensive understanding of the cost, performance, and ability to produce and manufacture the new components of the alternative architecture. Steps toward realizing that end begin with fully understanding and certifying across the community of stakeholders the intended set of demands that the proposed WFOV architecture will address.

Fully Assess Operational Performance of New Technology during Transition from Demonstrator to Prototype

The current CHIRP demonstration emphasizes assessing the validity of WFOV-expected simulations conducted during research, development, test, and evaluation (RDT&E) of third-generation infrared surveillance; additionally, it provides a baseline understanding of the basic performance of WFOV and integration of the payload on a commercial host. Evaluating test results over eight months to one year will help determine data accuracy and application of the WFOV sensor for missile-warning augmentation in the future. As discussed before, numerous data acquisition and processing areas need to be addressed as a means of determining whether the data acquisition and accuracies are sufficient to support missile-warning missions, both strategic and tactical. To validate data-accuracy capabilities, we will probably need a follow-on multisensor technology demonstration.

After establishment of performance requirements, sensitivity, WFOV uniformity, and defect rates, technology demonstration can move from validating expected performance of the WFOV technology to design demonstrations that more closely examine the specific mission-performance demands that the DOD assigns to the missile-warning augmentation capability. If augmentation is really intended to concentrate on enhancing resiliency of the most critical OPIR mission needs, then we should direct overall mission performance toward sustaining strategic and theater missile-warning capabilities through any contingency. We must demonstrate performance that supplies sufficiently accurate information to address missile warning through all threat environments across all geospatial areas. The architecture should focus on resiliency sufficient to survive a nuclear environment to the extent that other strategic forces can endure. To enhance the flexibility of the architecture, we must demonstrate WFOV sensor configurations that will extend the area coverage from one-quarter to full coverage of the earth, just as we must stiffen the bus and process multiple arrays together to ensure the accuracies necessary for OPIR missions. Moreover, we must deal with extended on-orbit satellite and sensor-life demonstration since replacement of short-life spacecraft or sensors for large, long-lived constellations significantly increases the life-cycle costs associated with providing the mission capability over time. After the demonstration of design technologies, missile-warning augmentation should move to the expected demonstration of an operational design configuration for the multisatellite prototype.

Validate Final Operational Performance and Production Costs during Prototype Development

Once final design for the missile-warning augmentation capability matures, we should pursue near-final-design prototypes to validate production and manufacturing costs and to develop production-line and supplier-tier organizations, processes, and costs. On-orbit assessment of multisatellite performance against near-standard designs will enable high-confidence understanding of constellation mission capability and substantiate the overall concept of deployment and operations. Additionally, confidence of the broader industrial base in estimates of production cost will assure the sustainment of program expenses throughout longer production runs of numerous satellites. High-confidence estimates of program costs will enable the definition of more realistic life-cycle costs for the entire architecture, thus enabling a better informed transition decision.

Understand the Architectural Implications

Finally, this low-risk approach gives us time to fully understand the entire architectural evolution (including ground) costs associated with transition to a "disaggregated architecture" of numerous individual spacecraft—both free flyers and hosted. Changes in operational concept and force management will have time to adapt to new ways of doing business. Understanding related costs for launch infrastructure, communications upgrades, mission management, mission data processing across many more systems, and mission-processing changes will all mature as the sensor and spacecraft design develops.

Acquisition History Reinforces Concern over Rapid Transitions

A number of reviews of space acquisition conclude that recurring risks continue to plague new starts of space programs and represent acquisition conditions that eventually lead to increases in program cost and unstable program-capability transitions. On 21 March 2012, Cristina T. Chaplain, GAO's director of Acquisition and Sourcing Management, testified before the US Senate Subcommittee on Strategic Forces, Committee on Armed Services, that

> our past work has identified a number of causes of acquisition problems, but several consistently stand out. At a higher level, DOD has tended to start more weapon programs than is affordable, creating a competition for funding that focuses on advocacy at the expense of realism and sound management. DOD has also tended to start its space programs before it has the assurance that the capabilities it is pursuing can be achieved within available resources and time constraints. There is no way to accurately estimate how long it would take to design, develop, and build a satellite system when critical technologies planned for that system are still in relatively early stages of discovery and invention. Finally, programs have historically attempted to satisfy all requirements in a single step, regardless of the design challenges or the maturity of the technologies necessary to achieve the full capability. DOD's preference to make larger, complex satellites that perform a multitude of missions has stretched technology challenges beyond current capabilities in some cases. Figure 2 illustrates the negative influences that can cause programs to fail.[11]

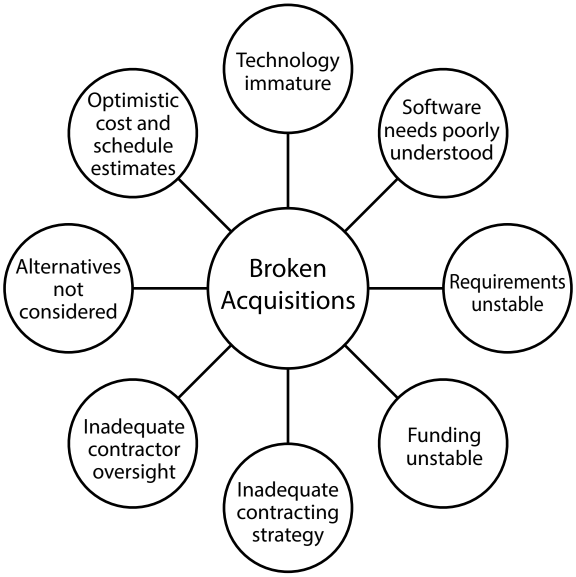

Technology immature
Optimistic cost and schedule estimates
Software needs poorly understood
Alternatives not considered
Broken Acquisitions
Requirements unstable
Inadequate contractor oversight
Funding unstable
Inadequate contracting strategy

Figure 2. Negative influences that can cause programs to fail

Similarly, in 2011 a National Defense Research Institute analysis of the root causes of recent breaches of the Nunn-McCurdy Amendment, designed to curb cost increases in weapons procurement, led RAND to identify the following lessons learned:

- Production delays increase exposure to changing private sector market conditions, which can result in cost growth.
- Acquisition flexibility (e.g., start-stop programs) comes with a cost.
- Cost estimates should be conducted independently of a program manager.
- Combining remanufactured and new build items causes complexity and can lead to cost growth.
- Greater planning of manufacturing process organization is required.
- Large reductions in procurement quantities can significantly increase per unit cost.
- Sufficient RDT&E is required to ensure the "produce-ability" of a program.
- Greater government oversight of the contractor is required in a technologically complex project.
- More "hedges" against risky elements of program are required.
- Additional collaboration is needed on design specifications and discussion of cost-performance trade-offs.[12]

None of this is new. The scar tissue of experience needs to inform the debate. Some of the proposed technologies under consideration as keystones for attaining disaggregated architectures have only just begun technology demonstrations to evaluate their performance capabilities, architectural implications (e.g., reduction of risk to individual nodes and mission network operation), and manufacturing/product feasibility. When only PowerPoint designs represent the extent of capability understanding, significant hazards remain that call for additional research and development and demonstrations to retire risk areas sufficiently to meet mission assurance needs. Structuring an affordable, time-sequenced approach toward retiring these problems will put into place the "hedges" to assure that we avoid unexpected program costs and realize expected performance within the larger architecture.

The complex DOD acquisition process has numerous stakeholders, complicated interrelationships among players, and inextricably linked, interdependent processes. Unsurprisingly, then, as program proposals transition from RDT&E demonstrations to full development and production, a host of new organizational structures, management processes, new personnel, and facility and equipment investment comes into play. The history of cost estimates made in response to requests for proposals suggests that those based on mature, well-known processes and structures are consistently more accurate than those based on fresh or untried approaches. Any assessment of risk during this transition should pay particular attention to the following areas of concern.

Control Requirements

With respect to OPIR, clear identification of the requirements subset that an augmentation program should provide will preclude confusion during transition to development and production. Clearly, the current demonstrated WFOV capabilities will not satisfy the full set of OPIR needs. Concentrating on the subset of requirements that such systems will augment alleviates requirements creep as the program progresses; it also hedges against the instability of program costs.

Improve Systems Engineering

The slow development of conceptual design by means of progressively more capable demonstrators builds better understanding of performance reliability, architectural integration, and manufacturing/production process costs. Structuring a low production rate allows time to evolve and adapt design and production processes incrementally so that design and production surprises do not result in major increases in program costs and schedule risks driven by operational imperatives.

Similar lessons apply to space systems and the transition from one space architecture to the next. To assure the retirement of similar risks to manufacturing feasibility, we must assure additional evolution from sensor and spacecraft demonstrators to prototypes. In the case of OPIR, the architectural implications of multisensory data integration and interleaving necessitate the testing of multi-WFOV sensors on-orbit to better comprehend the implications for data accuracy and fulfillment of the mission. Until we contend with such demonstrations and prototypes, the alternative architectures remain at high risk for the growth of program costs and possible mission failure.

Recognize Hidden Costs in Using the Commercial Base

The RAND study concluded that

> the broader lesson learned for this [Wideband Gapfiller Satellite] program is that when DoD procurement piggybacks on a commercial base, notably the commercial base of a particular company and its ecosystem, it takes a certain risk. The base may shrink, leaving it with less capacity to cover total overhead costs. Even if the base does not shrink, it will evolve. If DoD requirements do not evolve in parallel—and there is no inherent reason why they should—the divergence between DoD's requirements and the market's requirements means that either the requirements are compromised (admittedly, this may be acceptable in some circumstances) or, eventually, such programs have to stand on their own feet. . . . This suggests that a certain procurement discipline is called for, or DoD will pay the difference. Start-stop programs are costlier than steady-state programs (i.e., when buys are consistent from one year to the next), which, in turn,

> are somewhat more costly than total buy programs (e.g., we want six satellites, deliver them when you finish them). Although DoD cannot necessarily commit to even procurements for a variety of reasons (e.g., changing requirements, risk management, congressional politics), everyone concerned should understand that there are costs entailed in maximizing acquisition flexibility.[13]

Understand Changes in Procurement Quantities

Furthermore, according to the RAND study,

> Changes in quantity are never the primary source of a change in cost. Rather, quantity changes are always driven by some other factor, such as a change in threat or mission, which changes the requirement, or technical problems, which increase costs and therefore affect affordability.
>
> The initial reductions in planned quantities from the 32-ship class originally envisioned for [the] DD-21 [destroyer] to the ten ships included in the Milestone B baseline were due to affordability. As the system design matured and experience was gained with the key technologies and subsystems through the EDMs [engineering design modifications], more realistic (higher) cost estimates were developed, which reduced both the production rate (number of ships approved for construction in a given year) and total quantity.[14]

The current state of Earth coverage by the WFOV focal plane array will likely entail multiple sensors and spacecraft to offer coverage comparable to that of SBIRS. Because of this criterion and the imperative of enlarging constellation size to add a degree of resilience, architectural quantities will increase to 20 or more platforms. Should costs escalate in the transition from demonstration design to system-development decision, the effect on the DD-21 and other programs will likely apply in the missile-warning area as well. This risk again argues for a judicious demonstration and prototyping cycle to allow our understanding of design, performance, architectural, and production costs to mature.

Conclusion

Over the past few decades, Congress has paid particular attention to the DOD's program-acquisition difficulties and has repeatedly directed that both internal DOD reports as well as those by the GAO and various commissions review space and nonspace acquisition programs and practices. Those findings reinforce the need for a judicious development of technology together with incremental improvement and testing of designs prior to production commitment. In today's fiscal climate, setting aside these lessons to once again pursue an architectural transition based upon immature assessments of new technology performance and the ability to produce would be sheer folly. Furthermore, the consequences of delay or cost risks could prove operationally catastrophic for the missile-warning mission because, unlike previous circumstances, we lack a robust backup OPIR mission force structure that can sustain program disruptions. ✪

Notes

1. Lt Gen Ellen Pawlikowski, Doug Loverro, and Col Tom Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," *Strategic Studies Quarterly* 6, no. 1 (Spring 2012): 40–43, 47–48, http://www.au.af.mil/au/ssq/2012/spring/pawlikowski.pdf.

2. Sara M. Langston, "USAF Official: Long Road for Distributed Sats," *Aviation Week*, 31 August 2011, accessed 6 September 2011, http://www.aviationweek.com/avnow/news/channel_space_story.jsp?id=news/asd/20.

3. Director, Operational Test and Evaluation, *FY 2012 Annual Report* (Washington, DC: Director, Operational Test and Evaluation, Office of the Secretary of Defense, 2013), 275–76, http://www.dote.osd.mil/pub/reports/FY2012/pdf/other/2012DOTEAnnualReport.pdf.

4. Briefing, Space and Missile Defense Center, Huntsville, AL, subject: Theater InfraRed Proposed Joint Capability Technology Demonstration, 2011.

5. Air Force Space and Missile Systems Center/ Weather Program Office, Los Angeles AFB, El Segundo, CA, "Defense Weather Satellite Follow-on Industry Briefing," 25 April 2012.

6. SBIRS features a mix of four GEO satellites, two highly elliptical Earth orbit (HEO) payloads, and associated ground hardware and software, with dramatically improved sensor flexibility and sensitivity. Like its predecessor, SBIRS has sensors that cover shortwave infrared, expanded midwave infrared, and see-to-the-ground bands, allowing it to perform a broader set of missions than the DSP's. The HEO sensor configuration includes the following: an infrared payload of about 500 pounds (scanning sensor), three colors (shortwave,

midwave, and see-to-ground), sensor chip assemblies, Short Schmidt telescopes with dual optical pointing, agile precision gimbal pointing and control, passive thermal cooling, 100 Mbps data rate to ground, and strategic and theater surveillance. The GEO spacecraft configuration includes the following: predicted wet weight of about 10,000 pounds at launch; three axes stabilized with 0.05 degrees of pointing accuracy and solar flyer attitude control; RH-32 radiation-hardened, single-board computers with reloadable flight software; approximately 2,800 watts generated by GaAs solar arrays; Global Positioning System receiver with Selected Availability Secure Anti-Spoof Module; infrared payload of about 1,000 pounds (scanning and staring sensors); three colors (shortwave, midwave, and see-to-ground); sensor chip assemblies; Short Schmidt telescopes with dual optical pointing; agile precision pointing and control; passive thermal cooling; and secure communications links for normal, survivable, and endurable operations.

[7] Government Accountability Office, *Space Based Infrared System High Program and Its Alternative*, GAO-07-1088 (Washington, DC: Government Accountability Office, 12 September 2007), 3, http://www.gao.gov/assets/100/95166.pdf.

[8] Burdeshaw Associates, *Space Architecture Study* (Bethesda, MD: Burdeshaw Associates, March 2013), 181.

[9] Ibid., 151n3.

[10] Ibid.

[11] Senate, *Space Acquisitions: DOD Faces Challenges in Fully Realizing Benefits of Satellite Acquisition Improvements, Statement of Cristina T. Chaplain, Director, Acquisition and Sourcing Management, GAO, Testimony before the Subcommittee on Strategic Forces, Committee on Armed Services*, 112th Cong., 2nd sess., 21 March 2012, 15–16, http://www.gao.gov/assets/590/589487.pdf.

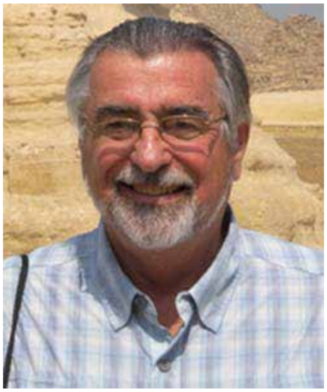
[12] Irv Blickstein et al., *Root Cause Analysis of Nunn-McCurdy Breaches*, vol. 1 (Santa Monica, CA: RAND Corporation, 2011), xvi, http://www.rand.org/content/dam/rand/pubs/monographs/2011/RAND_MG1171.1.pdf.

[13] Ibid., 84.

[14] Ibid., 27.

Jeffrey K. Harris

Mr. Harris (BS, Rochester Institute of Technology), the chief executive of JKH Consulting, LLC, has contributed to US national security capabilities in both government and industry where he has fostered new technologies and programs. He retired from Lockheed Martin as a corporate officer and served as president of Lockheed Martin Missiles and Space and of Lockheed Martin Special Programs. He also served as president of Space Imaging, the first company to provide high-resolution satellite imagery and information products for cost-effective solutions to global business needs. Before entering the private sector, Mr. Harris held senior national leadership positions, including assistant secretary of the Air Force for space, director of the National Reconnaissance Office, and associate executive director of the intelligence community. In all of these capacities, he provided direct support to both the secretary of defense and the director of central intelligence.



Gilbert Siegert

Mr. Siegert (BS, University of California–Santa Barbara; MBA, University of Wyoming) possesses more than 41 years of Department of Defense (DOD) and corporate aerospace experience in many of the space operations and systems that emerged during that period. He has 26 years of experience in the US Air Force, retiring as a colonel; 14 years in supporting the Office of the Secretary of Defense; and several years serving as the president of Space Ventures Consulting. During this consulting period, he worked for Burdeshaw Associates on numerous space-related projects. His expertise in space policy and strategy development, space program oversight, US government processes, and commercial space efforts contributed to the evolution of space operations over the last 40 years. While serving as a special assistant for space policy, strategy, and plans in the Office of the Deputy Assistant Secretary of Defense for Space Policy, Mr. Siegert was called upon to lead and participate in numerous congressional reports as well as interagency and DOD studies and analyses that directly resulted in organizational, program, and force-structure changes over the years. His analysis and inputs formed the basis for the space portion of the past several Quadrennial Defense Reviews and both Space Posture Reviews. He contributed to many of the foundational assessments that led to the Global Positioning System, various military satellite communication systems, space-based infrared system, electro-optical reconnaissance system, space-based radar, missile defense systems, Defense Support System program, multiple space launch vehicles, space situational awareness capabilities, and supporting technologies. Mr. Siegert's investigation of future commercial space capabilities such as commercial space launch ventures, space solar power generation technologies, space debris generation and domain consequences, and space traffic management concepts enabled him to contribute to space industry projections and industrial base analyses.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

Disclaimer

The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

http://www.airpower.au.af.mil

Public Health Considerations of Launching Nuclear Waste to the Sun

Dr. Murray R. Berkowitz

This article addresses the public health aspects of disposing of radioactive nuclear waste by launching it to the sun. The environmental and ecological problems that have occurred since British Petroleum's oil spill in the Gulf of Mexico on 20 April 2010 have prompted discussions about finding alternative energy sources. On 11 May 2010, Senator John Kerry (D-Massachusetts) and Senator Joseph Lieberman (I-Connecticut) introduced legislation (the American Power Act) "to secure the energy future of the United States, to provide incentives for the domestic production of clean energy technology, [and] to achieve meaningful pollution reductions."[1] Nuclear power, one of the many forms of alternative energy, has attracted renewed and increased interest. However, damage to the Fukushima Daiichi nuclear power plant from the 9.0 earthquake and subsequent tsunami in Japan on 15 March 2011, as well as reported problems at several nuclear power plants along the East Coast of the United States during Hurricane Irene, has heightened concerns about safety and health regarding the use of nuclear power. Furthermore, when power outages plagued the East Coast after "Superstorm Sandy" struck on 29 October 2012, the press ran articles about the issue of nuclear power plants endangering the public.

Nuclear waste material, which emits "ionizing radiation," poses a threat to public health, based upon the duration of exposure, distance to the source of radiation, type of radiation (e.g., alpha, beta, gamma, etc.), and the presence and type of any shielding.[2] Sources of radioactive nuclear waste materials include nuclear weapons, nuclear power sources, medical radionuclides used for diagnosis or treatment, radiation-producing machines, radioactive metals, and radioactive isotopes of all elements (usually found in "background radiation" exposures).[3]

The threat of exposure arises primarily from an accident or incident that results in a "spill" of radioactive nuclear material (i.e., a "nuclear spill") normally not encountered by the general (unprotected) population. Collection and containment of radioactive nuclear materials in secure sites—the current method of disposal—require safe transport and placement in specialized, secure installations. These repositories must be located away from populated areas; on installations whose physical security can be assured and where access by intruders—whether deliberate or inadvertent—is extremely unlikely and easy to detect (e.g., the Yucca Mountain Nuclear Waste Repository, which was defunded in 2010); and in places not likely to suffer from geological instabilities such as earthquakes, volcanoes, and so forth.

Another option is the collection and burial of radioactive nuclear waste material in the ocean, particularly in the deep crevices of mid-oceanic mountain ranges or extremely deep geologic formations such as the Marianas Trench. Clearly, any consideration of deep-sea burial would demand that the area be far removed from the oceanic tectonic plates—locations more subject to volcanoes, earthquakes, or other seismic geological activities. According to Charles Hollister and Steven Nadis, marine scientists feel that such places have not experienced geological activity for more than 50 million years and, therefore, will not likely become active in the future.[4]

Previous proposals for disposing of radioactive nuclear waste by launching it to the sun remove the threats of exposure from leakage of a storage facility or from the diversion of such materials by nuclear terrorists.[5] The underlying principle here is that all matter caught in the sun's gravity will lose its structural integrity due to the stress of gravitational forces and "break up" before reaching the sun. Moreover, high temperatures will incinerate and completely consume all matter prior to its reaching the sun's corona.[6] Specifically, as matter heats up, it expands beyond its structural integrity, and the heat energy encountered causes molecular bonds to break. Even the atomic integrity of elements of atomic number above two (i.e., helium) does not exist within the sun.[7] Essentially, the intense heat renders such elements into their composite subatomic particles (e.g., electrons, protons, neutrons, etc.).[8] Thus, the radioactive nuclear waste never impacts the sun, having no effect upon its "ecosystem," and therefore cannot "damage" the sun.

Magnitude of the Problem

In terms of the risk to public health, however, one must consider the possibility of a launch accident such as the destruction of a launch vehicle prior to leaving the earth's gravitation or its breakup shortly after launch, scattering radioactive debris. An examination of the US unmanned space program should reveal the likelihood of such an accident. Atlas, Centaur, Delta, Delta II, and Saturn V missions numbered over 1,000. Debris from accidents varied in size from centimeters to several meters in length and width, but none of it was radioactive. During the entire unmanned space program, the probability of an accident involving a space launch vehicle amounted to less than 3 percent.[9] Granted, the probability of such an occurrence is low, but it does exist.

We have long recognized the health risks presented by ionizing radiation. Witness the well-documented short- and long-term health issues associated with the atomic bombs dropped on Hiroshima and Nagasaki, the atmospheric tests of atomic and hydrogen bombs conducted by the United States and Soviet Union from 1946 through 1964, and the incidents involving nuclear power reactors at Three Mile Island in 1979 and Chernobyl in 1983. Risks associated with a launch vehicle carrying a payload of radioactive waste are analogous to those associated with nuclear fallout patterns observed during the atmospheric nuclear bomb tests until the advent of the Nuclear Test Ban Treaty.

Key Determinants

As mentioned above, the causes of potential public health problems are well known. Specifically, these include the biological effects of a radioactive nuclear waste environment on living organisms. Ionizing radiation can damage the biochemical, molecular, and cellular structures underpinning all life. Human behavior has no direct bearing upon this problem but can have an indirect effect in terms of safety and/or security concerns about the handling or containment of radioactive nuclear waste in the current international geopolitical milieu. That is, we must consider the possibility that such material might fall into the hands of terrorist groups which may use it to build and deploy low-yield "dirty" nuclear weapons (i.e., nuclear terrorism).

Making Policy and Setting Priorities

Again, one may dispose of radioactive nuclear waste material either by (1) sending it into space or by (2) collecting, isolating, and storing it on/under the land or deep within the oceans. Sending waste into space, especially launching it to the sun where it will burn up before reaching the corona, removes this hazard forever. As noted earlier, though, this option incurs the cost of launch vehicle operations and carries with it the risk of a launch accident that could spread radioactive debris unpredictably over a large geographic area. Collecting, isolating, and storing radioactive nuclear waste in or on the earth's land mass would be easy and inexpensive in terms of initial operations and logistics. Doing so, however, requires ongoing monitoring and security measures because terrorist groups could steal this material and put it to nefarious uses. Moreover, containment of the radioactive waste could become compromised by natural causes (e.g., earthquakes, volcanoes, etc.), leaking into the water table and contaminating land and/or water resources. Finally, disposal of this material deep in the oceans may prove just as costly as launching it into space. A maritime accident could subject the oceans near populated areas, fishing areas, and so forth, to radioactive contamination. Further, although a deep oceanic site is much more difficult to reach than a land-based containment facility, terrorists could still compromise its security and divert the radioactive material. Again, such a facility would require ongoing monitoring and security.

Regardless, we have the technical and scientific capacity to implement any disposal strategy, including launching payloads into space toward any target.[10] Political and social-behavioral obstacles to implementation arise from the public's perception of the risks associated with the production, use, and by-products of nuclear energy; in actuality, they are not as great as most of the public believes.[11] No published studies demonstrate that the health of workers in the nuclear industry is any worse than that of the general public, assuming observance of the appropriate safeguards. However, a failure to follow safe practices or the occurrence of an accident or incident involving nuclear materials can detrimentally affect the public health, especially in terms of producing cancers.

Regarding economic considerations, launching a payload into space costs about $10,000 per pound.[12] Thus, sending 100 metric tons of radioactive nuclear waste into space would cost $2.2 billion whereas storing it in the Yucca Mountain facility would have cost approximately $200 million per year.[13] Thus in 11 years we could fully amortize the cost of a space launch that carries much more waste than we could store at a single site on the earth's surface.

Space disposal of radioactive nuclear waste benefits individuals, communities, and society in general at the global level since this option removes the possibility of accidents/incidents during storage on the earth or the appropriation of material by terrorists. The attendant risks of space launch, noted earlier, involve incidents that could occur at or shortly after launch—or later but prior to leaving the atmosphere. Clearly, an accident at or shortly after launch would affect neighboring communities downwind of the site (e.g., Melbourne, Florida, near Cape Canaveral, and Patrick Air Force Base) where radioactive debris would quickly accumulate and compromise the public's health. According to a press release from Johns Hopkins University,

> Nuclear fallout arising from accident or terrorism contains radioactive iodine that can cause thyroid cancer, especially in babies and children up to 18. Potassium iodine tablets prevent the thyroid from absorbing radioactive iodine, protecting the gland.
>
> "Thyroid cancer historically has been a major public health problem resulting from nuclear incidents including the bombing of Nagasaki, Japan, and the nuclear accident in Chernobyl, Ukraine," says Paul W. Ladeson, M.D., director of endocrinology and metabolism at Johns Hopkins.[14]

Plans call for the distribution of potassium iodine tablets to people living within 20 miles of a nuclear incident.

If an accident occurred in the upper atmosphere, the winds aloft and prevailing jet streams would spread radioactive debris and affect populated areas, the number and location of which depend upon whether the incident took place in the northern or southern hemisphere. Moreover, the debris would disturb maritime life and commerce. Realistically, the impact of such an unlikely accident will be no worse than the results of any atmospheric nuclear bomb test, mentioned earlier, which entailed the detonation of multimegaton nuclear weapons that produced large amounts of radioactive debris in the form of fallout. The amount of nuclear waste material under scrutiny here does not fall into the "megaton" category.

Assessment of Related Risks

Several risk assessments (also known as environmental assessments) have a direct bearing on the collection and transport of nuclear materials, including issues of safety and analyses of the threat posed by potential accidents/incidents and their public health considerations. The National Nuclear Security Administration (NNSA) of the US Department of Energy has performed numerous such assessments. In January 2004, it concluded one that addressed the risks of latent cancer fatalities in the population resulting from the collection and transport of fissionable nuclear material—specifically, the movement by air of highly enriched uranium from Russia to a secure site near Knoxville, Tennessee. The NNSA performed assessments for cases of “no accident/incident,” for breakup or destruction of the aircraft in flight, for destruction on the ground (i.e., a “crash landing”), for destruction of ground vehicles transporting the materials (e.g., truck accidents), and for “no action.” In all cases and scenarios, the NNSA identified the worst one as a person “maximally exposed” to radioactive material at the site of a traffic accident on the ground, assessing the chance of a latent cancer fatality at “1.4 X 10^{-10}, or less than one chance in a billion.” For personnel handling the transfer of packages of highly enriched uranium from the aircraft to trucks, the chance was “less than 1 in 140,000.”[15] Consequently, the NNSA issued a finding of “no significant impact.” Similar risk assessments resulting in the same finding included those of the Chariton Valley Biomass Project, the decontamination and decommissioning of the nuclear reactor facility at the Argonne National Laboratory near Chicago, and the building of a nuclear-reactor fuels-materials facility near Aiken, South Carolina.[16]

Of special significance is the decision to fly the Cassini mission to Saturn in 1997, which has much relevance to the proposed idea. First, the mission involved the launching of a payload destined for other-than-earth orbit. Second, the spacecraft (i.e., the Cassini orbiter) is nuclear powered. Third, its payload, the Huygen probe, contains nuclear components. Risk assessments performed by the Interagency Nuclear Safety Review Panel for the National Aeronautics and Space Administration examined scenarios for launch accidents, accidental reentry into the earth’s atmosphere with the breakup and destruction of the space launch vehicle and payload, and accidental reentry due to the earth’s gravity during a “swing by” maneuver designed to increase the inertial velocity of the space vehicle during the interplanetary voyage phase. The Final Environmental Impact Statement for the Cassini Mission Report placed the median cancer fatality rate at “1.4 x 10^{-6}.”[17] This varies from “1 in 13 billion” to “1 in 280 billion.”[18] These accident/incident scenarios are notable because of their similarity to those that could occur with the proposed idea of launching nuclear waste to the sun.

Conclusion and Recommendation

This article has found that the risks to public health from disposing of radioactive nuclear waste by launching it to the sun are extremely small. Specifically, the median cancer fatality rate of one in 3.8 billion reported by the Cassini panel (based on scenarios comparable to those that might occur during the proposed launch)—and only in the event of an accident involving the space launch vehicle—is significantly less than the cancer fatality rate in the general population (one in 5,000). In light of the extremely minimal risks to public health, as well as the defunding of the previously proposed Yucca Mountain Nuclear Waste Repository, this article recommends that the United States reconsider the economically viable alternative of launching nuclear waste to the sun. ✪

Notes

[1] Senate, *A Bill to Secure the Energy Future of the United States, to Provide Incentives for the Domestic Production of Clean Energy Technology, to Achieve Meaningful Pollution Reductions, to Create Jobs, and for Other Purposes*, discussion draft, 111th Cong., 2nd sess., 11 May 2010, [1], http://www.kerry.senate.gov/imo/media/doc/APAbill3.pdf.

[2] "Radioactivity and Nuclear Physics," in Francis W. Sears and Mark Waldo Zemansky, *University Physics*, 2nd ed. (Reading, MA: Addison-Wesley Publishing, 1962), 901–16.

[3] C. L. Cheever, "Ionizing Radiation," in *Fundamentals of Industrial Hygiene*, 5th ed., ed. Barbara A. Plog and Patricia J. Quinlan (Itasca, IL: National Safety Council Press, 2002), 257–80.

[4] Charles D. Hollister and Steven Nadis, "Burial of Radioactive Waste under the Seabed," *Scientific American* 278, no. 1 (January 1998): 60–65.

[5] A. V. Zimmerman, R. L. Thompson, and R. J. Lubick, *Summary Report of Space Transportation and Destination Considerations for Extraterrestrial Disposal of Radioactive Waste*, NASA TM X-68211 (Cleveland, OH: Lewis Research Center, April 1973), http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19730012836_1973012836.pdf.

[6] Markus J. Aschwanden, *Physics of the Solar Corona: An Introduction* (New York: Springer, 2004), 26–29.

7. "Change of Phase," in Mark Waldo Zemansky, *Heat and Thermodynamics*, 4th ed. (New York: McGraw-Hill, 1957), 317–38; and "Applications of Thermodynamics to Special Systems," in ibid., 280–316.

8. "Spectra and Atomic Physics," in Sears and Zemansky, *University Physics*, 884–900.

9. Chuck Walker with Joel Powell, *Atlas: The Ultimate Weapon; by Those Who Built It* (Burlington, Ontario: Apogee Books, 2005), 265–78; Roger D. Launius and Dennis R. Jenkins, *To Reach the High Frontier: A History of U.S. Launch Vehicles* (Lexington: University Press of Kentucky, 2002), 102–46, 148–87; and Ed Kyle, "2013 Space Launch Report," 21 January 2013, http://www.spacelauchreport.com/log2013.html.

10. Edward M. Purcell, "Space Travel: Problems of Physics and Engineering," in *Models of the Atom*, ed. Richard P. Feynman (New York: Holt, Reinhart and Winston, 1968), 221–44; and Curtis D. Cochran, Dennis M. Gorman, and Joseph D. Dumoulin, eds., *Space Handbook* (Maxwell AFB, AL: Air University Press, 1985).

11. Eric Aakko, "Risk Communication, Risk Perception, and Public Health," *Wisconsin Medical Journal* 103, no. 1 (2004): 25–27, https://www.wisconsinmedicalsociety.org/_WMS/publications/wmj/pdf/103/1/25.pdf.

12. "Advanced Space Transportation Program: Paving the Way to Space," Marshall Space Flight Center, National Aeronautics and Space Administration, accessed 30 January 2013, http://www.nasa.gov/centers/marshall/news/background/facts/astp.html; David Kestenbaum, "Spaceflight Is Getting Cheaper, but It's Still Not Cheap Enough," National Public Radio, 21 July 2011, http://www.npr.org/blogs/money/2011/07/21/138166072/spaceflight-is-getting-cheaper-but-its-still-not-cheap-enough; Frank Sietzen Jr., "Spacelift Washington: International Space Transportation Association Faltering; the Myth of $10,000 per Pound," SpaceRef, 18 March 2001, http://www.spaceref.com/news/viewnews.html?id=301; R. L. Thompson, J. R. Ramler, and S. M. Stevenson, *Study of Extraterrestrial Disposal of Radioactive Wastes, Part 1*, NASA TM X-71557 (Cleveland, OH: Lewis Research Center, May 1974), 35, 37, http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19740014663_1974014663.pdf. (Note that 1974 costs were adjusted for inflation in December 2012.)

13. "Defense Nuclear Waste Disposal: Proposed Appropriation Language," in *FY 2000 Congressional Budget* (Washington, DC: Congressional Budget Office, 2000).

14. Karen Blum, "Johns Hopkins Conference to Study Prevention of Thyroid Cancer during Nuclear Events," press release, Johns Hopkins Medical Institutions, 26 February 2003, http://esgweb1.nts.jhu.edu/press/2003/FEBRUARY/030226.HTM.

15. Department of Energy (DOE) / Environmental Assessment (EA)-1471, "EA for the Transportation of Highly Enriched Uranium from the Russian Federation to the Y-12 National Security Complex," 15 January 2004, v, http://energy.gov/sites/prod/files/nepapub/nepa_documents/RedDont/EA-1471-FONSI-2004.pdf.

16. DOE/EA-1475, "Finding of No Significant Impact for the Chariton Valley Biomass Project Environmental Assessment," 10 July 2003, http://energy.gov/sites/prod/files/nepapub/nepa_documents/RedDont/EA-1475-FONSI-2003.pdf; DOE/EA-1483, "Environmental Assessment for Decontamination and Decommissioning of the Juggernaut Reactor at Argonne National Laboratory—East Argonne, Illinois," March 2004, http://energy.gov/sites/prod/files/nepapub/nepa_documents/RedDont/EA-1483-FEA-2004.pdf; and DOE/EA-0170, "Finding of No Significant Impact, Fuel Materials Facility, Savannah River Plant, Aiken, South Carolina," July 1982, http://energy.gov/sites/prod/files/nepapub/nepa_documents/RedDont/EA-0170-FONSI-1982.pdf.

[17] Solar System Exploration Division, *Final Environmental Impact Statement for the Cassini Mission* (Washington, DC: Office of Space Science, National Aeronautics and Space Administration, June 1995), 4-97 through 4-98, http://saturn.jpl.nasa.gov/spacecraft/safety/chap4.pdf.

[18] Ibid., 4-100 through 4-101.

Dr. Murray R. Berkowitz

Dr. Berkowitz (BS, Polytechnic Institute, New York University; MA, MS, Columbia University; MPH, Bloomberg School of Public Health, Johns Hopkins University; DO, College of Osteopathic Medicine and Surgery, Des Moines University Osteopathic Medical Center) is a tenured associate professor and director of preventive and community-based medicine at the Georgia campus of the Philadelphia College of Osteopathic Medicine and a Research Fellow at the Osteopathic Research Center in Fort Worth, Texas. He is residency trained in general preventive medicine and public health (State of Maryland Department of Health and Mental Hygiene). He is also board certified in neuromusculoskeletal medicine and osteopathic manipulative medicine as well as in preventive medicine and public health. Dr. Berkowitz holds added certification in occupational medicine. He served on active military duty as a Medical Corps officer in the US Army. Before attending medical school, he served in numerous assignments in the Army and Air Force. The scientific editor (editor in chief) of the *American Academy of Osteopathy Journal*, he is a published author and speaker with more than 100 manuscripts, papers, and presentations. Dr. Berkowitz is a graduate of the Armor Officer Advanced Course, Marine Corps Command and Staff College, Air Command and Staff College, and Air War College.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

Disclaimer

The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

http://www.airpower.au.af.mil

Predator: The Remote-Control Air War over Iraq and Afghanistan; A Pilot's Story by Matt J. Martin with Charles W. Sasser. Zenith Press (http://www.zenithpress.com), 400 First Avenue North, Suite 300, Minneapolis, Minnesota 55401, 2010, 320 pages, $21.00 (hardcover), ISBN 978-0-7603-3896-4.

On the most basic level, *Predator* is an exploration and illumination of the world of remotely piloted aircraft (RPA) through the lens of Lt Col Matt Martin's personal experience. He is particularly well suited to write a book about the MQ-1 Predator, having flown and supervised hundreds, if not thousands, of combat sorties with this system in both Operations Enduring Freedom and Iraqi Freedom, sometimes flying in both wars on the same day before going home to help his kids with their homework. "Professor" Martin, as his family sometimes calls him, uses his penchant for history and philosophy to eloquently tie intelligence operations and the role of RPAs into the broader context of the two wars.

The author shares much more than his combat experience with the reader, divulging personal struggles with the ethics of both remote combat and war in general. Martin has a knack for storytelling, and his true tales—told with conviction and packed with excitement, emotion, and well-developed characters—cover various roles and missions. He devotes much time to describing both friend and foe in depth. Indeed, the book reads more like a novel or collection of short stories than a dry journalistic recounting of events. I particularly valued the brief historical insights into Sunni-Shiite tensions and the description of the evolution of Iraq and Afghanistan. Martin provides abbreviated dossiers on Osama bin Laden and Saddam Hussein, explaining how they came to power and how their cultural and religious background shaped their despotic reigns. Although he does not source his information completely, it seems consistent with reports found in the mainstream media.

The author makes a point of addressing the myriad public misconceptions about so-called drones, arguing that these vehicles are in no way autonomous or unmanned. On the contrary, the operators simply fly them from a distance. RPA pilots and sensor operators get a much more detailed and persistent view of the damage they reap with their munitions, compared to pilots of faster platforms with less persistence. He asserts that for a given strike mission, firing a precision-guided Hellfire from a Predator causes far less damage than do heavier weapons dropped from fighters. The aircraft's low speed and high-fidelity optics also allow one to conduct battle damage assessment almost immediately. Martin draws on numerous, convincing anecdotes from his experience to advocate the employment of RPAs in tactical strike and close air support missions in addition to the vetted intelligence missions for which they were designed.

The author's perspective is certainly colored by his flying experience. A systems engineer, I expected to read more about some of the known problems with the MQ-1B system, especially those related to manpower, fatigue, and our nation's unquenchable thirst for RPA capabilities. The book briefly mentions some of the ergonomic issues with the controls and display system but largely ignores such matters. Further, although it examines the history of the RPA in combat, it fails to mention that, because of mission needs, the Air Force pulled the MQ-1B out of development before it reached full maturity.

I found *Predator* an exciting and engaging read that offered insights I didn't glean from formal interviews with other RPA pilots during my research on those platforms and human systems integration. I recommend this book to anyone who wants to learn more about RPAs and could benefit from firsthand accounts about flying them. People who speak out against the use of RPAs may find themselves challenged by *Predator* since it effectively argues for the proper employment of these aircraft.

1st Lt Travis J. Pond, USAF
Cape Canaveral AFS, Florida

Kantian Thinking about Military Ethics by J. Carl Ficarrotta. Ashgate Publishing Company (http://www.ashgate.com), Suite 420, 101 Cherry Street, Burlington, Vermont 05401-4405, 2010, 135 pages, $89.95 (hardcover), ISBN 978-0-7546-7992-9.

J. Carl Ficarrotta's *Kantian Thinking about Military Ethics* is a laudable book for readers seeking a refreshingly different perspective of Kantian ethics. A member of the Department of Philosophy at the United States Air Force Academy, the author approaches eight of the arguably most controversial ethical issues in an essay format. As indicated by the title, each stand-alone essay directly concerns the military, past and present, conveying what Kant thought or would have thought about the moral choices available.

The first essay, "Are Military Professionals Bound by a Higher Moral Standard? Functionalism and Its Limits," considers the presumption of military personnel being bound by a higher moral standard than the general populace due to the dictates of the *Uniform Code of Military Justice* in conjunction with expectations associated with the role of the military. "Women in Combat: Discrimination by Generality" explores the permissibility of discrimination against women, regardless of the pros or cons regarding their presence in combat. The third essay, "Careerism in the Military Services: An Analysis of Its Nature, Why It Is Wrong and What Might Be Done about It," perhaps the most widely applicable one in the book, addresses wrongs and corrections that occur daily. In the fourth piece, "Homosexuality and Military Service: A Case for Abandoning 'Don't Ask, Don't Tell,' " the author presents a strong case for repealing this highly controversial policy. Drawing on Ficarrotta's experience and expertise, "How to Teach a Bad Military Ethics Course" offers pivotal guidance about sharing or acquiring new knowledge about ethics.

The final three essays present cases dealing with war and its consequences: "Should Members of the Military Fight in Immoral Wars? A Case for Selective Conscientious Objection," "Does the Doctrine of Double Effect Justify Collateral Damage? A Case for More Restrictive

Targeting Practices," and "Just War Theory: Triumphant . . . and Doing More Harm Than Good." These pieces effectively elucidate these issues for readers unfamiliar with such ethical or philosophical matters as they relate to the military.

Reflecting the author's experience as an educator, each inviting and reader-friendly essay succinctly presents its case and allows for disagreement and dialogue. Unlike the textbook approach to military ethics and philosophy, Ficarrotta's study expands the application of Kantian and military ethics in their own right. Each piece also includes numerous references and additional commentary. From start to finish, the quality of these essays—"earlier versions of [which] have appeared or been presented elsewhere" (p. viii)—remains high.

For its impressive examination of the life-determining moral and ethical dilemmas that we face every day, I strongly recommend *Kantian Thinking about Military Ethics*. It offers a fine, fresh perspective of Kantian ethics and a thorough understanding of the world, our interactions, and the application of ethics in a military environment.

Jennifer Miller
Fort Bragg, North Carolina

Victory in Defeat: The Wake Island Defenders in Captivity, 1941–1945 by Gregory J. W. Urwin. Naval Institute Press (http://www.usni.org/navalinstitutepress), 291 Wood Road, Annapolis, Maryland 21402, 2010, 512 pages, $38.95 (hardcover), ISBN 978-1591148999.

The adage "Don't judge a book by its cover" perfectly applies to Gregory Urwin's *Victory in Defeat*. The title may lead some potential readers to dismiss the book as simply another treatment of World War II with a focus on US Marines or prisoners of war (POW). If that is the case, then they are missing a treasure trove that enriches the reader's soul. Urwin's extensive research brings his characters and a semblance of their experiences to life. Specifically, his interviews with several

American POWs and their Japanese captors, together with references to historical documents and other sources, lend vivid clarity to the scenarios and atrocities, making readers feel as if they were living in the moment.

The author's mastery of his subject shines through in objective descriptions of cultural influences, geographic landscapes, and perspectives derived from interactions with the people involved. The presence of extensive notes and references bolsters Urwin's scholarly credibility, and he remains up front and transparent concerning any research limitations that he might have encountered. His approach also highlights what many would argue is an ongoing battle in today's Air Force dealing with discrimination fueled by biases and selective attention. Ethnocentrism—both American and Japanese—contributed to barrier building. However, experiences revealed that individuals often dispelled the stereotype, enabling human compassion to work to the benefit of the Wake Island defenders (WID) and prison mates.

Leadership remains a key to breaking the stereotypes, especially if Airmen realize that they are both leaders and followers. The WIDs' decision to work as a team to guarantee survival and hope in a prosperous future should remain a call to arms for today's Airmen—not only to prevail in situations over which we have little control (e.g., the global economy, the engagement of state and nonstate actors, and political change) but also to develop effective strategies for our successors to implement.

Coupled with overcoming barriers such as gender, race, competitive categories, and age (a critical lesson learned from Urwin's themes) is the power of resilience, in terms of both the individual and the community. These themes mirror those found in the Air Force's Comprehensive Airman Fitness (CAF) concept. Adapted from the US Army's Comprehensive Soldier Fitness program, CAF initially sought to reverse the trend of suicides and suicidal ideations in the service. However, key players recognized the need to address underlying root causes to help individuals make good behavioral choices rather than continue conduct that produces suicidal thoughts or actions.

The collaborative approach used in developing CAF reflects the WIDs' efforts, both of which share the goal of becoming strong before, during, and after the emphasis on diversity. For example, although the WIDs were physically, mentally, emotionally, and socially resilient prior to capture, new circumstances that affected any one of those four areas resulted in greater reliance on social aspects to strengthen the other three. The healthier WID POWs shared rations with their weaker companions, and others offered to undergo punishment designated for POWs less able to endure it. Such selflessness reinforced a determination to survive and ensure that no one was left behind.

The Air Force's core values of "Service before Self, Integrity, and Excellence in All We Do" reverberated in my mind as I read this book. Just as the WIDs and others before us paved the way by using similar principles to serve our nation and humanity, so did the CAF concept synthesize our core values to build a foundation for overcoming uncertainty among individuals and the service as a whole. When sickness or execution reduced the number of WIDs, they abandoned their previously held biases in favor of ensuring survival of the group. Lessons learned from *Victory in Defeat* serve as a template that current and future Airmen can employ to hone individual skills, thereby strengthening the Air Force and allowing it to thrive under any circumstance.

Lt Col Katherine A. Strus, USAF
Peterson AFB, Colorado

Near Miss: The Army Air Forces' Guided Bomb Program in World War II by Donald J. Hanle. Scarecrow Press (Rowman & Littlefield Publishing Group) (https://rowman.com/Scarecrow), 4501 Forbes Blvd., Suite 200, Lanham, Maryland 20706, 2007, 368 pages, $76.00 (softcover), ISBN 978-0-8108-5776-6.

Operation Desert Storm's air campaign began at 2:10 a.m., Baghdad time, 17 January 1991. During the following days, television stations treated millions of people around the world to scenes of precision-guided munitions (PGM) hitting targets with near-pinpoint accuracy in "downtown" Baghdad and elsewhere in Iraq and Kuwait. The US Air Force had finally realized its long-sought-after but rarely achieved goal of precision strike. In a real sense, these modern air-to-surface weapons were the "grandchildren" of developmental weapons from various PGM programs initiated by Gen Henry "Hap" Arnold, chief of the US Army Air Forces (AAF) during World War II. Before the publication of Donald Hanle's *Near Miss*—the first in-depth, book-length treatment of these programs—very few people knew about these early attempts to develop PGMs.

Using organizational histories, records in the National Archives and those of the Office of Scientific Research and Development, World War II technical reports, and the personal papers of Arnold and Gen Carl Spaatz, supplemented by numerous secondary works, Hanle has produced a comprehensive history of the AAF's PGM programs of World War II. A retired US Air Force intelligence officer with a long and deep interest in airpower and World War II, he was a professor at the National Defense Intelligence University, Washington, DC, where he served as director of Terrorism and Asymmetric Warfare Studies and taught courses in intelligence analysis and military capabilities analysis. He also wrote *Terrorism: The Newest Face of Warfare* (Pergamon-Brassey's, 1989). In *Near Miss*, readers will see the author's intelligence background at work as he extracts data and information from technical reports and other sources, weaving the material into a scholarly yet easily read and understood account of General Arnold's PGM programs.

By mid-1943, a year after the AAF began bombing German industries, it had become evident to all but the most devoted advocates of high-altitude daylight precision bombing that the actualization of this doctrine did not even come close to the prewar boast that bombers with the Norden bombsight could place a 250-pound bomb into a pickle barrel from 20,000 feet. The reality of the air war over Germany—overcast skies, smoke from factories, German antiaircraft defenses, and a myriad of other factors—produced an average circular error probable of about half a mile (that is, half of the bombs dropped fell inside a circle a half of a mile in diameter, and the other half fell outside) with many bombs hitting the ground up to five miles from the designated target. By the end of the war in Europe in May 1945, the strategic bombing of Germany had killed between 350,000 and 700,000 civilians.

Because of this poor performance, General Arnold sought to improve bombing accuracy significantly and reduce collateral damage by developing various types of PGMs. By the end of the war, the AAF had experimented with glide bombs, vertical bombs (VB), jet bombs (JB), and war-weary bombers that used "primitive" radio and television control systems to direct the weapon to its intended target (Operation Aphrodite). Despite the money, effort, and Arnold's personal influence and effort, these programs had produced very little by the end of the war: the VB-2 Azimuth Only (AZON), used with limited success in Holland and Burma by September 1945; the VB-3 Range and Azimuth Only (RAZON), used with limited but good success in the Korean War; and the JB-2 "Loon," an American version of the German V-1 "buzz bomb," a prototype that became the ancestor of the US military's cruise missile programs.

In his book, Hanle examines every major PGM program that the AAF developed during the war. He first presents the origins of the general PGM program, mainly the fruit of General Arnold's personal efforts to obtain weapons with significantly greater accuracy than contemporary gravity bombs. Arnold hoped that their expected combat use would speed up the destruction of German industry, limit collateral damage, and reduce aircraft and aircrew losses—goals sought by today's air leaders. The author discusses the research, development, and combat employment (what the Air Force now calls operational testing) of each weapon system in sufficient detail but without devolving into minutiae. Finally, he offers an extensive discussion of the reasons for the general failure of these early PGM programs. Consequently, readers will acquire a thorough understanding of the origins, development, and problems of Arnold's programs.

Hanle correctly cites three main reasons for the general failure of the "primitive" PGM efforts. As the reader might suspect, the most significant reason involved the rudimentary state of technology for the radio- and television-control systems. Today's PGMs utilize satellites, computers, microprocessors, laser beams, digital networks, and circuit boards to achieve pinpoint accuracy—sophisticated technology not available in the 1940s when radios used fragile vacuum tubes and copper wiring. Second, the author discovered significant resistance to the PGM program from operational commanders who generally saw these "Buck Rogers fantasy weapons" lying outside accepted strategic bombing doctrine and wartime operational practice, generally considering them a waste of resources. Finally, he found that the success and momentum of these programs depended, to a significant degree, on Arnold's personal interest and involvement (especially so, given the resistance from the operational commanders to the PGM programs), which many design developers saw as meddling.

In summary, *Near Miss* is an outstanding and scholarly, yet highly readable, history of the AAF's PGM programs of World War II, perhaps the last major subject of this war to remain unexplored from unclassified documents. Until several years ago, I knew only about the JB-2 Loon and Operation Aphrodite. (President John F. Kennedy's oldest brother Joseph died when his radio-controlled and explosive-filled B-24 prematurely exploded on 22 August 1944.) Then in July 2005, I became an Air Force historian at Eglin AFB, Florida, where the AAF conducted much of the testing for these first-generation PGMs, and learned more about them from the material in the Air Armament Center's history office. Thus, from a historical, professional, and personal perspective, it was exciting to discover that someone had finally written about this previously almost forgotten aspect of World War II that portended so much, once the technology and the commitment to pursue the development of PGMs became available after the late 1960s.

Dr. Robert B. Kane
Maxwell AFB, Alabama

The B-45 Tornado: An Operational History of the First American Jet Bomber by John C. Fredriksen. McFarland & Company (http://www.mcfarlandbooks.com), 960 North Carolina 88, Jefferson, North Carolina 28640, 2009, 272 pages, $45.00 (softcover), ISBN 978-0-7864-4278-2.

John Fredriksen spent years reading after-action reports and unit histories as well as meeting with veterans to pull together an interesting and comprehensive study of the North American B-45, the first jet-powered bomber. Overshadowed by other aircraft, it remains relatively unknown yet holds numerous firsts in Air Force operations and reconnaissance. Ordered during the final months of World War II after the US Army Air Forces encountered the Luftwaffe's Arado 234 jet bomber in 1944, the B-45 entered the inventory in 1949.

The book recounts the challenges of bringing new technologies and an innovative aircraft into service. For example, jet engines, still in their infancy, presented problems—witness the B-45's General Electric J-57s, which caught fire or blew up in their wing-mounted pods. Additionally, the aircraft's APQ-24 radar system had tubes that required aligning by hand before it functioned properly.

The B-45A bomber was designed to replace the World War II–vintage B-25, but funding cuts during the Truman administration forced the Air Force to curtail the buy of B-45s in order to pay for the B-36. Consequently, Tactical Air Command (TAC) used this light bomber to meet a proposed interdiction role. As atomic bombs became smaller and lighter and as the United States began to fear possible Soviet encroachments into Western Europe and the North Atlantic Treaty Organization (NATO) in the 1950s, the Air Force modified 40 B-45s and then sent them to Royal Air Force (RAF) Sculthorpe in the United Kingdom to give US Air Forces in Europe a boost during the Cold War. Operating under trying weather conditions, the jet bombers laid the foundation for the quick-action alert and NATO exercises that would become keystones in the following decades.

The reconnaissance version of the aircraft, the RB-45C, purchased to supplement the vulnerable RB-29 and RB-26, proved a greater operational success during the Korean conflict and later in the first overflights of Russia, China, and Korea. The RB-45C shifted between TAC and Strategic Air Command (SAC) to meet needs and overcome capability shortfalls within the Air Force and during the war in Korea. The 33 aircraft, assigned to the 91st Strategic Reconnaissance Wing, rotated to RAF Sculthorpe and Yokota Air Base and Johnson Air Base in Japan. Their Manchurian, Russian, and Chinese overflights were fraught with danger, and a MiG-15 shot down an RB-45C on 4 December 1950. The B-45 and RB versions had only limited tail-gun capabilities; they also lacked warning devices, leaving them vulnerable to rear-hemisphere attacks. Using radar and optical cameras, the RB-45C monitored the introduction of Chinese forces to North Korea and the growth of MiG fighter forces in China, Manchuria, and Russia—the so-called sanctuary areas. The first air-refuelable jet bomber in the US inventory, the B-45—as well as the reconnaissance versions—could take on fuel from KB-29 and KC-97 tankers. The range extension for the RB-45C allowed it to penetrate the Soviet Union and fly reconnaissance sorties all the way to Kiev from the United Kingdom.

In 1952, when the RB-47 began to arrive in force with SAC, the RB-45Cs were refurbished and then joined TAC's 19th Tactical Reconnaissance Squadron, serving in the 47th Bomb Wing alongside the B-45, deployed to the United Kingdom. Both the bomber and reconnaissance versions disappeared from the Air Force inventory in 1958. Some survivors soldiered on in research and engineering test roles until the early 1970s.

Well researched and replete with interesting facts such as beer-can repairs and the loan of RB-45Cs to the British RAF to fly Russian penetration sorties in 1952, *The B-45 Tornado* will astonish readers with its accounts of difficulties and challenges encountered by everyone associated with the bomber. Veterans' loyalty to the aircraft helped the author capture even the smallest details. This book, the only one on the market about the B-45, is a must-read for bomber and Cold War enthusiasts.

Gilles Van Nederveen
Fairfax, Virginia

The Art of Air Power: Sun Tzu Revisited by Sanu Kainikara. Air Power Development Centre (http://airpower.airforce.gov.au/), TCC-3, Department of Defence, Canberra ACT 2600, Australia, 2010, 461 pages, $28.50 (hardcover), ISBN 9781920800345.

Composed some 2,400 years ago, Sun Tzu's *The Art of War* is recognized as the oldest surviving treatise on military strategy—the starting point for all that has since been written on the subject. Always of great influence on Chinese military thought, this work received less attention in the West until the 1960s when growing interest in irregular warfare inspired the seminal English-language translation of the late Brig Gen Samuel B. Griffith III, USMC. Today, English-speaking readers may choose from among some 200 translations of this ancient text.

The Art of War is a model of concision. Barely 40 pages long in English translation, it is written aphoristically, consisting of 13 short chapters in which Sun Tzu offers maxims about how to prevail in war, preferably without fighting. In many ways a virtue, the extreme brevity of *The Art of War* is also a hindrance to understanding. That is because Sun Tzu confines himself to offering conclusions and does not share the thought process upon which they are based. The result is a series of terse prescriptions for victory that are timeless but unexplained.

Here is where Sanu Kainikara's *The Art of Air Power* comes in. Where Sun Tzu is succinct, Kainikara is prolix; where Sun Tzu offers unexplained conclusions, Kainikara elucidates—frequently at length—on the probable reasoning behind them. In a word, *The Art of Air Power* is not simply another addition to the existing shelf load of translations of *The Art of War*. Instead, it is an extended exegesis that seeks to explain the meaning of Sun Tzu's precepts within a contemporary military context, with special emphasis on their implications for airmen. The author's credentials suggest that he is up to this ambitious task. A former fighter pilot and a retired major general who served in the Indian Air Force, Sanu Kainikara is the author of seven books on airpower and a long-time student of Sun Tzu. Holder of a PhD in international politics from the University of Adelaide, he serves as deputy director for strategy at the Royal Australian Air Force's highly regarded Air Power Development Centre.

Kainikara's thesis asserts a strong congruence between Sun Tzu's prescriptions for victory and the capabilities of modern airpower. In support of that contention, he offers a chapter-by-chapter analysis of *The Art of War*, explaining how the ancient wisdom of Sun Tzu can be tapped to usefully inform employment of the air weapon. Emphasizing airpower's flexibility and adaptability, the author argues that whether used independently or in concert with other arms, airpower is the instrument nonpareil for fulfilling Sun Tzu's exhortations about achieving speedy victory at the least possible cost, overcoming the enemy by wisdom and not by force alone, avoiding strength and attacking weakness, and shifting rapidly between direct and indirect approaches.

At more than 400 pages of text, *The Art of Airpower* is a long read and closely argued. But it will amply reward airmen and others willing to persevere. Some occasional discursiveness notwithstanding, the book offers a thorough, thoughtful, and compelling analysis of the affinities between airpower and the timeless injunctions of Sun Tzu.

Readers will also appreciate Kainikara's subtitles, which employ the terminology of contemporary conflict to identify the focus and importance of what follows. The same may be said of the author's "one-liners." Interspersed throughout the text, these doctrine-like assertions encapsulate in a few well-crafted words what the preceding pages have argued at length.

Two critical observations: the unfortunate lack of an index reduces this book's value as a reference tool, and although Dr. Kainikara does provide a bibliography of his sources (all of them of good repute), scholars may wince at the absence of footnotes. That said, this reviewer commends *The Art of Air Power* to students and practitioners of airpower alike—especially those who teach it or write airpower doctrine.

James Titus, PhD
US Air Force Academy

Leading the Narrative: The Case for Strategic Communication by Mari K. Eder. Naval Institute Press (http://www.usni.org/navalinstitutepress), 291 Wood Road, Annapolis, Maryland 21402, 2011, 152 pages, $24.95 (hardcover), ISBN 97816125110477.

Strategic communication is an important, difficult subject to grasp. Commanders, junior officers, and noncommissioned officers have to consider many factors when they communicate, especially outside the military, because that process can have either a favorable or detrimental effect on the public's perception of a military organization or a response to an operation. Mari Eder tackles this complex idea, offering the reader a strategic communications primer, albeit through a decidedly military perspective. Her years of service in various Army public affairs roles and depth of experience in the joint environment shine through as she discusses ways that military communication has worked and can improve, as well as military leaders' opportunities to take advantage of effective communication.

One might think that *Leading the Narrative*, at only 152 pages, would be a quick read. However, Eder includes a number of complex concepts regarding strategic communications, succinctly describing many ideas and backing them up with good analysis. The first chapter, "Military Media Relations," offers a good foundation and introduction, especially for professionals not associated with public affairs. Subsequent chapters pay particular attention to strategic communication, defining ways to identify deficient areas and improve communication, and others detail the value and role of ethics for the military professional who deals with the media. Summing up the importance of ethics, she closes one chapter by observing that "the soldier is America's cowboy in the twenty-first century, a role model of service and ethical behavior" (p. 76), a vivid characterization of the military juxtaposed to society as a whole. Throughout, Eder highlights the importance of ethics and the public's opinion of the military—both critical to establishing effective strategic communication.

Although many sections of the book provide valuable insight into the need for good communication, some need improvement. For example, chapter 3, "Strategic Communication and the Battle of Ideas," and chapter 4, "Toward Strategic Communication," both discuss the role of public affairs at the outset of Operation Iraqi Freedom in 2003—and do so in almost identical fashion, sharing paragraphs and concepts. The author should either consolidate them or choose another example to represent her ideas. Furthermore, the section "Public Affairs Career Field Redesign, 2013–14" in chapter 10, "Challenge to Change: Developing Leaders for the Twenty-First Century," could have concluded the book quite effectively; unfortunately, Eder makes it extremely Army-specific, taking the form of a tactical-level, service-centric discussion. A higher-level example—one that applied the concepts of the book, especially in the joint environment—would have proved more useful.

Despite these issues, readers will discover material that they can apply to their professional careers. It is extremely important not to become caught up in the immediate needs and visceral reactions to media operations but to look forward to beneficial second- and third-order effects. Failure to address the strategic results of our communication can impair our ability to carry out military operations efficiently.

Overall, the noncommunication professional should find *Leading the Narrative* well worth exploring. The many key elements of communication can assist military members at all echelons. Strategic communication, an important part of the operating environment in the twenty-first century, could be lost among the required tactical- and operational-level education and training that encompasses most military members' time.

Maj Benjamin L. Carroll, USAF
Joint Base McGuire-Dix-Lakehurst, New Jersey

Let us know what you think! Leave a comment!

Disclaimer

The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

http://www.airpower.au.af.mil