ASPJ

Air & Space Power Journal

Vol. 35, Issue 3

Fall 2021

75 Years
B-52 Stratofortress

ASPJ AIR & SPACE POWER JOURNAL

Front Cover Illustration by Mr. Jim Stovall: *"B-52G,"* 1985

Air & Space Power Journal
600 Chennault Circle
Maxwell AFB AL 36112-6010
e-mail: aspj@au.af.edu

Visit *Air & Space Power Journal* online at https://www.airuniversity.af.edu/ASPJ/.

The *Air & Space Power Journal* (ISSN 1554-2505), Air Force Recurring Publication 10-1, published quarterly in both online and printed editions, is the professional journal of the Department of the Air Force. It is designed to serve as an open forum for the presentation and stimulation of innovative thinking on military doctrine, strategy, force structure, readiness, and other matters of national defense. 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, the Department of the Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

https://www.af.mil/ https://www.spaceforce.mil/ https://www.aetc.af.mil/ https://www.airuniversity.af.edu/

SPECIAL FEATURE

SENIOR LEADER PERSPECTIVE

STRATEGIC COMPETITION

TECHNOLOGY

BOOK REVIEWS

FROM THE EDITOR

Welcome to the Fall issue of *Air & Space Power Journal (ASPJ)*. Our contributions include a special feature on the B-52, a senior leader perspective discussing unmanned aerial systems, a forum focused on two aspects of strategic competition, and a technology forum considering topics including satellite control, directed-energy weapons, science and engineering career fields, and mosaic warfare.

Our issue begins with a tribute recognizing the earliest anniversary date of the B-52, the acceptance of the prototype by the US Army Air Forces in June 1946. The special feature includes a brief timeline and personal stories from current and former operators.

Our *Senior Leader Perspective*, a contribution from Brigadier General Houston R. Cantwell entitled "Piloting Unmanned Aircraft with a Computer Mouse," considers several challenges posed by data-link interruptions. Brigadier General Cantwell offers his perspectives on the implications of decreased human oversight in the operations of these systems.

In our *Strategic Competition* forum, Dan Morabito proposes a unified definition, taxonomy, and theory of victory for information warfare in "National Security and the Third-Road Threat." In "Combatting Russian Influence through Improved Security Assistance," Walter Richter discusses ways in which US security assistance mechanisms can counter Russian influence as countries transition from Soviet-legacy defense systems to US-produced systems.

Our *Technology* forum features four contributions. In "Shifting Satellite Control Paradigms," Carl Poole, Robert Bettinger, and Mark Reith argue that with the advent of megaconstellations, improvements in cybersecurity are vital. In "Directed-Energy Weapons," Alfred Cannin explains how directed-energy weapons can provide a direct targeting capability throughout escalation-of-force timelines yielding less collateral damage, fewer civilian casualties, and increased opportunities for de-escalation. Brian Fry advocates for a change in Air Force personnel policy that would better operationalize and reward the knowledge and skills of active-duty scientists and engineers in "Mobilizing Uniformed Scientists and Engineers." Our forum closes with an article by Jörg Schimmelpfennig, "F-35 O-Ring Production Function versus Mosaic Warfare," that engages the O-ring production theory to argue mosaic warfare, given realistic scenario parameters, tends to improve substantially the chances of successful missions.

Team *ASPJ* hopes you find our fall issue informative and insightful.

~The Editor

Special Feature: The B-52 Stratofortress

Seventy-five years ago in June 1946, the US Army Air Forces awarded Boeing a contract to build the XB-52, the world's first intercontinental bomber.[1] After several modifications, the Air Force, satisfied with the design, ordered 13 B-52As in 1952.[2] On the occasion of this particular anniversary of the Stratofortress, *Air & Space Power Journal (ASPJ)* is pleased to highlight some aircraft milestones followed by a few first-hand accounts of crew members.

Acquisition and activation. Production moved quickly; the first flights of the B-52Ds, B-52Es, and B-52Fs occurred annually from 1956 to 1958. In the middle of these "firsts" in 1957, the Air Force approved the contract for the next-generation B-52, the B-52G. The greater fuel capacity meant an increased range of 30 percent; the tail gunner seat was moved adjacent to the electronic counter measures operator; and a welcome climate control feature was introduced—essentially dual-zone.[3] In 1960, the B-52H, still in operation today, made its first flight. In total, from the XB-52 to the B-52H, 774 aircraft were approved, produced, and fielded in just over 10 years. The Air Force retired the B-52Ds in the early 1980s and retired the B-52Gs following the Gulf War in 1991.

Strategic power projection. Under General Curtis E. LeMay, the B-52 flew nonstop flights as far north as the North Pole (1956), and in 1957 in Operation

Power Flite, three B-52Bs became the first jet aircraft to circumnavigate the globe nonstop, completing the flight in just over 45 hours. In early 1962, the Stratofortress conducted a nonstop flight between Japan and Spain that broke 11 speed and distance records.[4] The Strategic Air Command's B-52s were a global alert force—on the ground and in the air—ready to conduct nuclear counterstrikes in the event of a Russian attack.

Weapons capability. The 1950s also saw the successful fielding of air-launched cruise missiles (ALCMs), one of which—the Hound Dog—remained in service until 1977. During the 1980s, the B-52 began to carry nuclear-armed ALCMs; an early GPS system and the advent of terrain contour mapping allowed these missiles to navigate autonomously.

The Air Force also deployed Harpoon antiship missiles from the B-52Gs and B-52Hs in the early 1980s. That same decade, the Air Force converted a number of ALCMs to carry a conventional payload. These conventional ALCMs—CALCMs—were first employed during Operation Desert Storm. The Stratofortress has had an aerial mining capacity for decades as well, and in 2019, the Air Force revealed work on arming B-52Hs, the most recent model, with Quickstrike air-dropped sea mines.[5]

The B-52 was first used to carry conventional ordnance in the Vietnam War in missions executed under an operation code-named Arc Light. While most missions during the war were blanket bombardments, the B-52 also provided direct tactical support to the Army and the Marine Corps. During the Vietnam War, the B-52 also gained its well-known moniker, the BUFF—short for Big Ugly Fat "Fellow."[6] During Operation Niagara in 1968, B-52s dropped 75,631 tons of bombs around Khe Sanh in over 2,700 sorties. In support of Operations Linebacker I and II in 1972, Strategic Air Command increased its deployment of B-52s to 210; the entire fleet at the time numbered 402.

During the execution of Linebacker II, Sergeant Samuel Turner made history as the first tail gunner to shoot down an enemy aircraft—in this case, a MiG-21. Airman 1st Class Albert Moore later duplicated Turner's feat, and Moore's aircraft, "Diamond Lil," still graces the north entrance of the US Air Force Academy in Colorado Springs.[7] Linebacker II, also known as the "Christmas Bombings," from December 18–29, 1972, saw more than 15,000 tons of bombs dropped, 15 B-52s shot down, 8 crewmembers killed, 24 crewmembers deemed missing in action, and 33 crewmembers captured and later returned. Linebacker II led directly to the negotiated peace settlement the following year that enabled President Richard Nixon's "Peace with Honor." The aircraft had proven itself once and for all as a key operational asset during wartime.[8]

Post–Cold War. In the early 1990s, the Stratofortress was again called to battle. In the opening days of the Gulf War in January 1991, seven B-52s conducted the longest strike mission in history to date: a 35-hour, nonstop flight totaling 14,000 miles. During the war, the B-52 was used to attack ground forces as it had in the Vietnam War. Accounts of Iraqi troops, much like North Vietnamese troops almost 20 years before, tell the tale of the terrifying impact of a B-52 bombing run.[9] The Gulf War also saw the B-52 operate from bases in countries such as Saudi Arabia, the UK, Turkey, and Spain.[10]

In 1991, President George H. W. Bush cancelled the B-52 crews' 24/7 strategic alert, and two years later, the aircraft was adapted to carry the next generation of conventional weapons. The Stratofortress went to war again in 1999, with the Serbian armed forces the next adversary to experience the terror of a B-52.

Partner missions. One variant of the aircraft, the NB-52B or *Balls Eight*, carried the winged and manned, air-launched X-15 supersonic aircraft for its 199 flights from 1960 to 1968. While used for other programs in the interim, the Air Force's *Balls Eight* relationship with hypersonic aircraft came full circle—the aircraft's final mission was as the mothership for the X-43A, an unmanned hypersonic research vehicle. *Balls Eight* was formally retired from service in December 2004 after an illustrious 44-year career.[11]

Twenty-first century adaptations. In 2014, the Air Force introduced the first B-52s equipped with the Combat Network Communications Technology system, providing operators with "communication data links, full-color LCD displays with real-time intelligence feeds overlaid on moving maps," and in-flight capabilities to retarget weapons and mission parameters.[12]

Discussing the 2020 decision by the Air Force to keep 76 B-52Hs in service until 2050, Air Force Chief of Staff General Charles Q. Brown said of the challenges and opportunities of the almost 60-year-old Stratofortress, "it is like an old truck that was built when they actually build them tough. . . . The challenge you have with a platform like that now is how to bring in new technology and capability."[13]

Originally purchased for $6 million each, B-52Hs can fire long-range missiles—including hypersonics that can travel up to 1,000 miles—nuclear-tipped cruise missiles, satellite-guided bombs, and air-dropped mines. In 2020 and 2021 to date, B-52s have flown strategic power-projection missions to the Persian Gulf, Ukraine, and the western Pacific as well as support missions to Afghanistan. Colonel Anthony C. Cain, USAF, retired, and a former B-52 navigator, sums it up appropriately below: "The B-52 and its generations of crews, maintainers, and support personnel are symbols of the United States Air Force's global strike capability. The professionalism and dedication shown by anyone who has been connected to the mission makes the BUFF legendary."

In this one of many anniversary years of the Stratofortress, *ASPJ* is honored to highlight a few observations and stories of current and former B-52 crew members.

Exalt 15. September 3, 1975, started out as a routine B-52G training flight day. Our crew arrived at the 51st Bomb Squadron building about 0900 to take our photo for the squadron crew line-up. Our crew of seven (with a new pilot along for training) went to base operations, filed our flight plan, and proceeded to the aircraft to ready it for take-off. The regular copilot was to fly in the instructor pilot's seat.

Take-off from Seymour-Johnson AFB, North Carolina, was uneventful, but as we were climbing on departure, the instructor pilot, flying as the co-pilot, told us we had a fuel leak in the right wing. We declared an emergency to air traffic control, did all our fuel-leak emergency procedures, informed our command post of the problem, and canceled all training activity in order to burn off fuel to land safely.

The fuel leak was under control, and everything was normal as we did some routine checks of the flight and navigation systems. At 1221, everything changed. Somewhere near Aiken, South Carolina, the aircraft started shaking violently, worse than any turbulence, and pulled forcefully to the right, twice. It felt like a car driving from smooth pavement to very rough railroad tracks. We determined later that it was probably the right-wing tearing, the autopilot trying to correct the aircraft to counter the additional wind resistance, and the right wing continuing to fail. In a matter of seconds, the aircraft rolled right. The pilots realized inverted flight was imminent and ejected at approximately 120 degrees of roll, the electronic warfare officer and radar navigator after them. The electronic warfare officer's seat worked as advertised, but while the radar navigator's seat got him out of the aircraft, it did not automatically separate from him. Our gunner was out of his seat at the time and did not eject.

I was the navigator on that flight, and the accident board determined I was the last one out. I remember forcing my head to look for the radar navigator, but he was gone, and debris was streaming out of the hole where he was sitting moments before. I strained to get my legs in ankle restraints. which was necessary because we were in downward ejection seats, but the accident board theorized my ejection was up. The board theory was the aircraft had already exploded because my hatch was black from fire burns, while the others were white. I finally pulled my handle and remember thinking, "oh my God, I'm dead." Then everything went dark. Because of that, I believe God does not let you see when you are going to die. You are shielded from that experience. I did see my life flash before my eyes in snippets of memories.

The next thing I knew, I was in a parachute. The chute was tangled with the strap from my ejection seat, which failed to separate as expected. To land safely, I had to pull the seat to me and stand in it to control it. Ironically, the seat helped me penetrate through a pine forest. I managed to get out of the parachute harness and get my survival radio, even though I was beat up from the ejection and the seat banging into me. By then, aircraft were looking for downed crewmembers. Minutes later, I contacted one by twice radioing, "Downed crewmember, Exalt 15." He directed helicopter rescue who found me soon thereafter.

The pilot who was receiving training was in the helicopter. He told me the radar navigator had not survived. As it turned out, our downward seats were damaged by the torquing action. The radar navigator did everything right, but the aircraft exploded near enough to knock him unconscious. The copilot in the instructor pilot seat, and the gunner did not survive the aircraft explosion. I lost three friends and brothers that day.

Hector Marquez, USAF, retired,
navigator, BUFF: 1975–81; 1989–92

Proud gunner. I enlisted in the United States Air Force in 1975. I was trained as a nuclear weapons specialist (463X0), and my first assignment was to the largest nuclear weapons storage site on the planet, Manzano Mountain, Kirtland Air Force Base, New Mexico. My work as an Airman included a stint as a volunteer at the National Atomic Museum and Sandia Labs to maintain the displays of assorted inert nuclear devices.

There was a B-52 "B" model 52-0013 at the museum on display that was fully intact but "locked." I found the keys to the front hatch and helped myself to a tour of the inside all the way back to the gunner's station. I was so impressed with that war machine that I set a goal to retrain and fly as a gunner! I was accepted, and I loved every minute of it! I am proud to be one of the last B-52 gunners!

Senior Master Sergeant James M. Ryles, USAF, retired,
T-1 gunner, WST gunner, instructor gunner, and evaluator gunner, BUFF: 1975–91

B-52 gear fire and saga of Slip 57. May 2006. We had just landed 18 hours after the end of my last combat sortie at a certain island location. We landed with a full load of retained GBU-31s, and the drag chute failed, so the pilots had to get on the brakes a little more aggressively than normal. We taxied to the weapons' check area to have our bombs pinned, and the pilots set the brakes and cleared the weapons' troops in. My radar navigator and I were watching the marshaller in the forward-looking infrared when he suddenly began making an infinity symbol with his wands. Confused, we kept watching him. Next, he began making motions like "take off your shoulder straps." Not recognizing any of the motions, the crew debated what he was trying to tell us: bees? Miller time? We quickly realized it was bad when his third action was to throw down his wands, spin, and begin running away at full speed. (As we found out later, the hydraulic line going to the front right main landing gear had popped, pouring hydro fluid all over the hot brakes. Of course, it lit on fire, producing flames that went over the top of the wings).

The entire crew realized things were bad at exactly the same instant, and the radar navigator had already opened the entry hatch before the pilot was able to yell "Egress" twice. Unfortunately, he had forgotten to remove his headset, so I watched his head snap back as the comm cord reached the extent of its length. Realizing what had happened, the radar navigator grabbed the comm cord connector, unsuccessfully gave it two or three pulls before yelling "forget this," ripping off his headset, and jumping out through the open hatch. I, after watching all this while patiently sitting in my seat, jumped up and ran to the hatch, only to have this entire comm cord issue and resolution myself.

As I hit the ground, I momentarily froze and looked up at the fire. Then I spun and began running. My electronic warfare officer later told me that he knew it was bad when he saw me freeze. The rest of the crew quickly followed, and we were all having our own foot race down the taxiway.

As we all stood together huffing and puffing, watching the fire being extinguished, we were in the perfect position to watch a B-1 land directly in front of us (we were headed home, and the B-1s were replacing us). It was after dark as I watched him on final approach. I remember seeing wing-tip lights, white lights where the wings sweep but definitely noticed no landing lights. (On the tower radio recording, it actually has them calling the tower "Slip 57, with the gear.")

My brain was running a little slow after the adrenaline of the emergency egress we had just completed, so I began to analyze what I was seeing—no lights mean no gear, which means. . . oh, crap. The B-1 flew a very stable approach, and a beautiful flare, right up until his burner cans started dragging the ground. The aircraft suddenly made a hard pitch over and slammed the rest of its body onto the ground. All of us standing there on the parallel watching this happen directly in front of us said "shit" simultaneously.

I fully expected the aircraft to explode, so my first thought was to get down. Unfortunately, there was nothing to get behind, and I knew that being inside the fireball, it would do no good, so I decided that if this was going to be my last sight, I was going to enjoy it instead of cowering. Luckily, it did not explode and instead began to travel more than a mile down the runway on its belly. I watched a spiraling red-orange flame follow the jet as it slid. After a second, I realized that I'd probably live, but the B-1 guys were probably dead, so I just kept watching.

After it came to a stop, we all yelled, "get out guys!" Right then, a Maintenance bread truck roared up, threw open their door, and the driver yelled, "get in!" We all piled in on top of each other, and the driver peeled out as the seven or eight of us began to try to untangle ourselves. While we were driving away, the B-1 crew was trying to egress. They later claimed that they didn't realize they were gear up until they tried to drop the entry hatch, it fell about 6 inches and stopped—uh-oh. The weapons systems officers in the back then popped one of their top hatches to egress. There is a warning in most aircraft tech orders regarding the escape rope: "ensure that the rope is fully extended before use." The weapons systems officer on this jet evidently forgot, so he just grabbed the end of the rope and jumped. Thankfully, he was the ONLY person hurt during either accident. He didn't slow down until he hit the pavement, hurting his back substantially but in doing so extended the rope for the rest of the crew.

Major Kyle "HoBBS" Holt, USAFR,
navigator and instructor radar navigator, BUFF: 2003–present

Longevity. In 1975, while talking with the crews on alert, a vice wing commander of the 28th Bomb Wing commented that the BUFFs would fly so long that he feared his grandson would fly them some day. Little did he know that he might have been talking about a GREAT grandson!

Lieutenant Colonel Alan W. Debban, USAF, retired,
navigator and instructor radar navigator, BUFF: 1973–85

Professionalism and dedication. In the last decade of the Cold War, B-52 crew duty tended to revolve around flying and alert duty. Depending on the unit mission and the size of the unit, crews would be assigned week-long alert tours one or two times each month. In between alert tours, flying training missions provided opportunities to practice the full strategic strike profile—takeoff, air refueling, low-level penetration and bombing (often with simulated short-range missile launch), high-altitude navigation (usually with a celestial navigation leg to simulate loss of navigation systems), simulated cruise missile launch, instrument approach, and pattern work to keep pilots proficient at landing the airplane. Training schedules alternated between alert tours to ensure crews were current and proficient at both day and night flying. Low-level routes included mountainous and nonmountainous terrain. The sorties could last more than 10 hours if the assigned low-level routes were far from the takeoff base.

Alert provided opportunities to keep current with tactical doctrine, emergency war order procedures, and simulated flight profiles for units with simulators. Alert facilities were self-contained with crew sleeping, dining, and recreational facilities. Crews could leave the facility to attend meetings, simulator training, or to visit the base exchange or other authorized facilities, provided they had a radio that could receive transmissions from the unit and Strategic Air Command command posts.

At northern bases, like the one where I spent my first tour, winter months provided the possibility of snow . . . feet of snow. During one alert tour, the snow turned into a three-day blizzard that closed the base. Not just slowed traffic . . . no traffic. Snow plows were useless—as soon as they made a pass, the snow filled in the gap as if the plow had never been there. Soon, road crews gave up and decided to wait out the storm. Nothing moved on the installation while everyone watched the snow fall.

The problem for those of us on alert that week was that we depended on the dining facility for our meals. By the third day, every drink and snack choice in the vending machines was gone—even the stuff that never sold! We had tried to open the refrigerators in the kitchen, but they were padlocked, and the facility manager did not have the key—only SSgt B, the cook, had the key to the food!

On the morning of the fourth day, several of us were gathered in the dining hall watching through the large picture window as the snow continued to fall. Someone shouted, "Hey, look at that!" Across the pristine field of snow that now made up the northern perimeter of the base was a solitary figure, arms at shoulder height, looking like a swimmer, plowing through an ocean of white. We realized it was SSgt B headed our way! Word spread quickly through the facility that we were not forgotten. As SSgt B made his way, half-frozen, into the facility, a crowd of bomber crews, tanker crews, maintainers, and security forces personnel lined down the hall to cheer him on.

Someone said, "SSgt B . . . what were you thinking? You could have frozen to death out there!" Looking through his thick, iced-over glasses, he replied, "I figured you guys were getting hungry, and I had the key to the fridge." He had half-walked, half-swum from his home on the other side of the base—about five miles in freezing temperatures. When the Strategic Air Command inspection team came, to no one's surprise, SSgt B was identified as a top performer—because, of course, that's what he was.

B-52 duty in my experience was all about teamwork. The airplane was, and is, a crew airplane that requires coordination to produce mission success. Every individual on the installation was somehow tied to the mission. Our leaders made sure everyone knew how they contributed and that everyone was important to the success of the mission, right down to SSgt B, the alert chow-hall cook. We trained hard, worked hard, and celebrated unit, crew, and individual successes. We believed that deterring nuclear aggression was vital to our national security, just as it still is in today's challenging world. The B-52 and its generations of crews, maintainers, and support personnel are symbols of the United States Air Force's global strike capability. The professionalism and dedication shown by anyone who has been connected to the mission makes the BUFF legendary.

Colonel Anthony C. Cain, USAF, retired,
navigator and radar navigator, BUFF 1982–93:

Old dog, new tricks. The mighty B-52 Stratofortress soldiers on. The original Air Force leaders and Boeing engineers who designed and fielded this fine aircraft could never have envisioned this workhorse's staying power. They probably would be equally impressed with the BUFF's longevity and relevance as a valuable asset in America's strategic arsenal. Time and again, the BUFF has answered the nation's call. I am grateful I had the opportunity as a crew dog to contribute a small part to the BUFF's already legendary history. From flying into combat after 9/11 to pushing the limits of hypersonic research and everything in between, this weapon system is not complete without her crew and maintainers. My best experiences in the BUFF will always be associated with great Airmen who demonstrated extraordinary teamwork.

During the first X-51 Waverider hypersonic launch in 2010, we took the jet to an altitude of 50,000 feet and performed a successful launch. It was the latest chapter demonstrating the BUFF's versatile role supporting aerospace research at Edwards Air Force Base, California. It was an exciting day at the office, and it would not have happened without exceptional performances from everyone involved. In retrospect, our trusty B-52 and crew once again met the challenge, provided a threshold for future BUFF modifications, and helped advance America's technological edge.

I characterize the BUFF just like Han Solo described the Millennium Falcon, "She may not look like much, but she's got it where it counts." There's no other aircraft like this built to last, and there may never be another that will even come close. The B-52 is a great enabler in more ways than one, and it brings out the best in many Airmen—past, present, and future.

Lieutenant Colonel Sean "GW" Celi, USAF, retired,
instructor radar navigator, BUFF: 1999–2011

Thrilled with the job. I flew as a navigator and radar navigator for seven years at both Ellsworth (77th Bomb Squadron) and Griffiss (668th Bomb Squadron) in the later 1980s. Here's a part of a letter I wrote to my parents that I discovered while cleaning out the belongings of my late father. I was 28 and thrilled with my job.

First 1988 Strategic Air Command Bomb Comp mission—June 1988

"Flew all the way out to Red Flag—11.5 hours round trip! Talk about tired! It was a good mission—we got jumped by a couple of F-15s right after we entered the route, but we dove into the mountains, and all they got were a couple of IR passes. My gunner locked 'em up twice, so we'll see how it turns out.

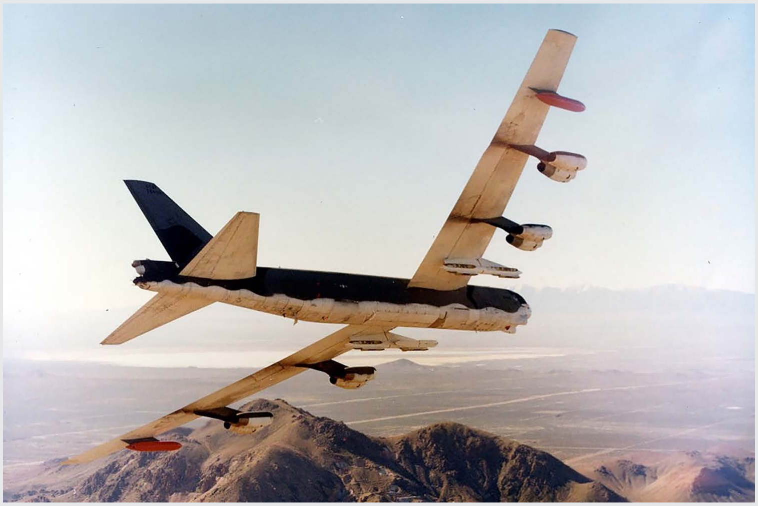


Figure 1. B-52 descends to low level upon entry into its training route

The bomb run was pure chaos! They set up surface-to-air missiles all along the approach to the target, and the EW had us all over the sky "avoiding" the threat. All the while, I'm trying to aim on radar and zero out our timing. My Nav was sick as a dog, so I'm flailing away doing three things at once! Evidently, things worked because the pilots said we flew right over the target, and we released within a second of our assigned time.

The wing commander met our plane when we finally landed and wanted to know how we did. Who knows?—We're flying 370 kts at 500 feet . . . it's hard to judge if you put it on target or not. So, I lied and said it was a "Shack." Made him feel good. Oh well, one more to go."

Maintenance representatives, Sgt. Wayne T. Smith, 416th Munitions Maintenance Squadron, Sgt. William B. Pendergast, 416th Avionics Maintenance Squadron, SrA. Paul A. Towers, 416th Organizational Maintenance Squadron and TSgt. Joseph B. Kneece, 416th Field Maintenance Squadron. Second row, 668th Bomb Squadron members, Capt. Steve B. Thomas, Capt. John J. O'Brien, Capt. Bryan M. Branby, 1st Lt. David J. Re, SSgt. Earl E. Babcock. Third row, 1st Lt. David W. Brown, Capt. Kenneth L. Swab, *Capt.* Bernard T. O'Rourke, 1st Lt. Vincent C. Abel and TSgt. Ricky L. Hollins, not pictured—*Maj.* James A. Blackwood, 1st Lt. Shawn E. McManigell.

Figure 2. Photo of maintainers and flight crew during the late 1980s

Lieutenant Colonel Bryan Branby, USAF, retired,
navigator and radar navigator, BUFF: 1983-90

Notes

[1] Tara Copp, "B-52 Engine Replacement Could Keep Bomber Flying through Its 100th Birthday," Defense One, June 30, 2021, https://www.defenseone.com/.

[2] "B-52 Stratofortress, Historical Snapshot," Boeing (website) n.d., https://www.boeing.com/.

[3] Bill Yenne, *B-52 Stratofortress: The Complete History of the World's Longest Serving and Best Known Bomber* (Minneapolis: Zenith, 2012), 45.

[4] "Historical Snapshot," Boeing.

[5] David Axe, "To Stop a Chinese Invasion, B-52s Could Drop Mines in the Taiwan Straits," *National Interest* (blog) July 4, 2021, https://nationalinterest.org/.

[6] Yenne, *Stratofortress*, 86.

[7] Don Branum, "Records Detail MiG Kill by 'Diamond Lil' Tail Gunner," US Air Force Academy Public Affairs, December 24, 2010, https://www.usafa.af.mil/.

[8] Yenne, *Stratofortress*, 91–99.

[9] Yenne, *Stratofortress*, 87, 130; and Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 201, 247.

[10] Yenne, *Stratofortress*, 126–27.

[11] Yenne, *Stratofortress*, 69–78.

[12] "Historical Snapshot," Boeing.

[13] Michael R. Gordon, "For Wars of the Future, Pentagon Looks to Distant Past: The B-52," *Wall Street Journal*, January 25, 2021, https://www.wsj.com/.

Piloting Unmanned Aircraft with a Computer Mouse

Challenges to Point-and-Click Flying

Brigadier General Houston R. Cantwell, USAF

Flying an aircraft using a keyboard and mouse has its advantages, but it has its challenges too! Having grown up at the controls of the nimble F-16, I have had to fundamentally adjust my mindset while flying the modern RQ-4D Phoenix, a Global Hawk derivative. While flying the F-16, I certainly never worried about going "lost-link." Relying on a vulnerable data link introduces challenges to safe and effective flight operations.

Additionally, unmanned aircraft incorporate unprecedented levels of automation. In most circumstances, the automation reduces pilot workload and improves effectiveness, but in some instances, the pilot must override the automation to maximize safety or mission effectiveness. As militaries expand applications of unmanned technologies, several lessons learned here at the NATO Alliance Ground Surveillance Force may prove instructive.

Data-link interruptions. The first edict of operating any unmanned aircraft is that the data link will be interrupted (normally at the most inopportune time); consequently, the pilot must always anticipate the aircraft's immediate actions. Typically, this is called the lost-link profile or flight plan. In this situation, the aircraft may be programmed to turn, descend, or change airspeed but often will proceed to a predesignated holding area to wait for restored communications. Challenges in this scenario include weather events in the holding area or the introduction of a new surface-to-air threat.

Pilots must therefore remain vigilant, constantly updating lost-link flight plans to preclude the aircraft from performing actions that jeopardize safety or survivability. Once communications are interrupted, the aircraft will only perform those actions for which it was programmed. If the aircraft was programmed to hold for three hours and then return to base but only had two hours of fuel remaining, it will diligently maintain its holding pattern until it impacts the ground due to engine failure and fuel starvation. Maintaining updated lost-link flight plans is essential to flying unmanned aircraft safely.

Delays in executing the lost-link plan can also cause the aircraft to fly in an unintentional manner. During near-border operations, mitigating this issue becomes a priority. In my F-16, maps, GPS, and, as a last resort, an aggressive, 90-degree, 4-to-5g pull on the stick kept me from accidentally venturing into prohibited airspace—I have avoided a North Korean or Pakistani airspace incursion using this reliable maneuver. But the RQ-4D, operating at altitudes over 50,000 feet and bank angles under 20 degrees, moves differently, often requiring a turn radii of more than 5 miles. When intelligence, surveillance, and reconnaissance collection requirements force near-border operations, the possibility of accidental airspace incursion is real.

Although manually maneuvering the aircraft via mouse clicks and waypoints is intuitively easy, severed communication links create heightened tension when every mile counts. The RQ-4D has multiple redundant links. Normally redundancy improves reliability, but transition to alternative links is not seamless. Precious time may elapse before the aircraft successfully receives the command from the pilot—a less-than-ideal process during near-border operations. As the aircraft attempts to regain communications with the pilot through alternative links, it is flying at 350 knots on a flight plan based on the pilot's last input, making an unintentional incursion into a foreign country a very real possibility.

One mitigation technique involves manually shutting off all backup data links thus making it clear the aircraft is either receiving immediate input on the primary link or taking action by performing its lost-link profile (which in this case would be an immediate turn away from the border), thus minimizing the chance of a border incursion.

Pilot overrides. Like any unmanned system, the RQ-4D computer bases its decisions on information collected through onboard aircraft sensors (pilot-static system) or information provided through data links. The two most important data links in this case are GPS and the primary aircraft control link to the pilot. The aircraft sensors permit the machine to remain safely airborne with little assistance from the pilot—basic aircraft control, airspeed, turns, climbs, and descents are easily accomplished without additional input.

Yet aside from basic aircraft control, pilot input is necessary. Border awareness, threat awareness, fuel awareness, and aircraft system degradation—these are areas where the aircraft lacks automated awareness. The machine relies on human input (and thus a data link to the pilot) to maximize safety and effectiveness. For example, the RQ-4D lands itself. When crosswinds are high or visibility low, this auto-land feature is ideal. As the landing phase is the most critical, the aircraft will ensure its systems are optimized for a safe touchdown. If it suspects a nonoptimum inertial navigational system navigation solution, approach angle, or fuel imbalance, it will execute an automated go-around.

In some instances, however, this logic is deliberately overridden by the pilot. If icing is encountered during decent, the pilot inhibits the auto-go-around function. This action precludes an auto-go-around and subsequent climb and/or holding pattern within dangerous icing conditions. The pilot always maintains a "manual" go-around command if the aircraft ever appears to be in an unsafe position to land.

Looking ahead. Certainly, through additional sensors, links to external databases, and a real-time interface with other machines, the RQ-4D *could* greatly reduce its dependence on human input. But in my experience, the cost quickly becomes prohibitive. Each additional set of automatic inputs, new sensors, or machine-to-machine connections requires millions of dollars of investment to ensure the capability and then to certify the capability as "airworthy." Unlike ground unmanned systems, airborne systems require airworthiness certification, thus incurring additional costs.

Two challenges to operating and developing unmanned aircraft are worth noting. First, the importance of data-link assurance during the employment of any unmanned system cannot be overstated. Mission effectiveness will be degraded whenever communications are interrupted. War fighters must commit to improving link reliability across the battlespace. The *2020 Department of Defense Electromagnetic Spectrum Superiority Strategy* raises several important issues, but much more work is required. Second, what processes are worth automating? Technology exists to automate more—the aircraft could certainly be engineered to stay within assigned borders or avoid surface threats—but the war fighter must determine which processes are worth the money to automate. Keeping a human in the loop is often less expensive.

The operational success of unmanned systems hinges on a fundamental criterion, namely, how to provide an aircraft's mission computer sufficient information to make proper decisions within a dynamic environment. As demonstrated by the RQ-4D, unmanned aircraft rely on information provided by onboard sensors and data links—critically, those with GPS and with the pilot.

When data links are denied, the aircraft must be programmed to perform in a safe, effective, but most of all, predictable manner. Future systems tasked with more complex mission sets (the use of lethal force) will rely on an increased amount of information exchanged across an even greater number of data links—the location of friendly forces, enemy forces, threats, and weather. As the number of data links increase and mission complexity increases, the challenge to ensuring safe and effective operations, regardless of link status, becomes ever more difficult.

For the foreseeable future, the successful use of unmanned systems in combat operations necessitates careful integration of computer-driven processes and human oversight. Ultimately, data-link vulnerability and aircraft logic management (manipulating aircraft decision calculi to maximize overall effectiveness) are growing challenges that remain fundamental to mission effectiveness when physically separating the war fighter from the machine. ✪

Brigadier General Houston R. Cantwell

Brigadier General Cantwell is commander of the NATO Alliance Ground Surveillance Force at Italian Air Base, Sigonella, Italy.

National Security and the Third-Road Threat

Toward a Comprehensive Theory of Information Warfare

Daniel Morabito*

Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.

Giulio Douhet, *The Command of the Air*

The United States is losing an information war with its competitors. China and Russia have attacked the United States for decades, costing our country billions of dollars. These activities have sown division, extremism, and violence among the American people, and undermined societal norms and democracy. Despite this national security threat, the US government remains poorly organized to employ its information instruments of power. The US military in particular lacks a unified theory, definition, doctrine, and organizational structure for information warfare (IW).

Early Information Advantage

Information has been a vital component of warfare since the earliest recorded battles. In the 1469 BC Battle of Megiddo, the Hyksos King of Kadesh, who led a revolt of Palestinian and Syrian tribes against the Egyptian pharaoh, Thutmose III, was missing critical information as to the disposition of the Egyptian army.[1] Anticipating an Egyptian attack on the stronghold city of Megiddo, the Hyksos king assessed the large Egyptian army would likely approach using one of two larger roads to the east and west of the city, and he divided his forces to intercept them. Using information gained from his scouts and discerning that the rebel leaders expected him to approach by these two broad roads, Thutmose instead chose a third, narrow road that led to the south of the city.[2]

The pharaoh's advisors begged him not to use this road, as it was only 30 feet wide in places with heights on either side that would invite an enemy ambush. Had the rebel army chosen to acknowledge their vulnerability and position themselves defensively on this third road, they would have had a tremendous

*A version of this article first appeared as a three-part series in Over the Horizon, the digital journal of the USAF Air Command and Staff College.

advantage. They might have defeated the Egyptian army or forced them to withdraw. Too late, and with their army divided and focused to the east and west, the rebels "realized that their enemy had done the thing they had not calculated on and had surprised them."[3]

The pharaoh's early information advantage and the rebel army's failure to acknowledge the third-road threat allowed the Egyptians to establish a positional advantage relative to large portions of the rebel army that were then caught outside their city and cut off from reinforcements. It also enabled a cognitive advantage—surprise—over the occupants of the city and the divided army outside. The Egyptians, using their positional advantage gained through information advantage, overwhelmingly defeated the divided army, laid siege to the city, and captured it.[4]

When news of the rebel army's crushing defeat reached the remaining Mesopotamian cities that had not yet joined the rebellion, they were deterred from joining the Hyksos king and voluntarily sent tribute to Thutmose indicating they did not want war, further evidence of how actions in the information environment reverberate throughout other domains to influence attitudes and behaviors. Having forged its reputation as a military power at the Battle of Megiddo, Egypt established itself as the regional hegemon for the next two decades.[5] This, the first recorded battle of history, illustrates how the interplay of information across all domains contributes to decisive effects at the tactical, operational, and strategic levels. Furthermore, it reveals the ability of information to establish advantages across other instruments of power.

The Enemy Lies at Your Fingertip

> *The skillful leader subdues the enemy's troops without any fighting; he captures their cities without laying siege to them; he overthrows their kingdom without lengthy operations in the field. . . . Without losing a man, his triumph will be complete.*
>
> Sun-Tzu, *The Art of War*

Military power projection as a function of information, distance, and geography has shaped the character of war from the first recorded conflicts to today.[6] As warfighting technology evolves, the speed at which a combatant can traverse space and attack an adversary has increased tremendously, with each conflict and technological advancement altering the character of war.[7] Given recent advances in high-speed network connectivity and information technology, geography and distance no longer protect the United States from direct and persistent information-based attacks. The global trend toward faster data transfer across increasingly connected devices—the so-called internet of things—means adversaries now maintain a presence in American homes, delivered through smartphones and other technology.

Within this rapidly evolving information environment, China and Russia are waging information wars against the United States calibrated to advance their national interests while avoiding direct and decisive military conflict with the West. Their strategies center on exploiting America's emphasis on free speech and freedom of the press which, by constitutional mandate, may not be infringed except under extraordinary circumstances. Consequently, the information environment competitive space is ill-suited for Department of Defense (DOD) intervention, exposing a gap in civilian and military thinking about how to defend the nation.

The US military's power comes from those it represents—the attitudes, knowledge, and beliefs of the American people are a national center of gravity and strategic concern. A consequence of the deluge of competing adversarial narratives, delivered by America's enemies through the internet of things, is that many Americans cannot discern between fake news and truth. This flood of narratives leaves the population misinformed, uncertain, and prone to attitudes, knowledge, and beliefs shaped by social media filtering and bias.[8]

Simultaneously, the American military prioritizes preparing for large-scale combat operations to deter near-peer military competitors and, if conflict occurs, to win decisively.[9] This focus leaves the Department of Defense ill-prepared and poorly postured to counter peer competitors in the information environment, lacking doctrine, an organization, and even a definition for information warfare. Meanwhile, America's enemies use the ubiquitous connectivity of the internet to bypass the country's traditional military defenses, directly and maliciously sowing division and mistrust among the American people on an unprecedented scale.

The US government must aggressively pursue social, legal, and organizational change to counter these enemies within the information environment. To do this effectively, it must understand how IW is used against the United States today as well as how it may be used in the future. While the US government struggles to understand and counter this form of warfare, the Department of Defense must buy time for US democracy to adapt to this new fight by developing a unified theory of information warfare that robustly informs how it competes both within the information environment and across the continuum of military conflict.

Information Warfare Theory

> *The aggressor is always peace-loving (as Napoleon Bonaparte claimed to be); he would prefer to take over a country unopposed.*
>
> Carl von Clausewitz, *On War*

Using information for military advantage is as old as the earliest recorded battles, yet defining the phenomenon as a type of warfare has proven frustratingly elusive.[10] The phrases information warfare and information operations (IO) are often used interchangeably, with little clarity as to what they mean and how they manifest across the competition continuum.[11] Joint doctrine provides no definition for IW and defines IO as "the integrated employment, during *military operations*, of *information-related capabilities* in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own [emphasis added]."[12] This definition is lacking as it constrains IO to "military operations" and describes the phenomenon using presupposed "information-related capabilities."

Similarly, the US Air Force recently described information warfare as "the employment of *military capabilities* in and through the information environment to deliberately affect adversary human and system behavior and preserve friendly freedom of action during cooperation, competition, and conflict [emphasis added]."[13] This description is also lacking because it defines IW based on presupposed "military capabilities."

Both definitions describe IW and IO from military perspectives within the system they seek to understand. This is a mistake as, according to military theorist John Boyd, "one cannot determine the character or nature of a system within itself."[14] Such efforts generate confusion and disorder, ultimately impeding action and magnifying friction. As a result, both definitions do little to illuminate how the United States and others might compete within the information environment using novel capabilities across the continuum of military conflict.

The US military lacks a sufficient, comprehensive doctrinal understanding of IW, resigning IO to a mere tertiary function supporting the primary focus of large-scale combat operations. For example, the December 2020 release of Joint Publication 5-0, *Joint Planning*, makes only a single reference to information operations, describing it as an example of "requested military flexible deterrent options" without elaborating on what that means or how it should be integrated into Joint planning.[15]

Joint Publication 5-0 makes meager efforts to include information environment considerations during Joint planning by adding a statement that "the Joint force synchronizes operations in the information environment to shape the perceptions, decisions, and actions of relevant actors" and adds "information environment (including cyberspace), and electromagnetic spectrum" considerations within the course-of-action development step of the Joint planning process.[16] Meanwhile, China and Russia have already operationalized IW theory and integrated it into their operational art, considering information warfare sufficient in its own right to triumph in competition below the threshold of armed conflict.[17]

United States military doctrine must define IW based on the phenomenon's basic elements and emergent properties. Such a definition will inform capability development and employment based on the broader nature and character of the information environment, rather than unnecessarily constraining IW thought to expressions of preexisting military capabilities.

The next section posits a theory of IW from its most basic elements through its implementation as a weapon used to support national interests. It reveals IW as a manifestation of the Clausewitzian clash of wills expressed through competing narratives and shaped by access, trust, and cognition.[18] The section concludes with a proposed novel information warfare taxonomy, definition, and theory of victory.

Constructing Knowledge

In order to define information warfare, one must understand how data, information, and knowledge interact within information ecosystems to create individual and shared perceptions of reality. Data, the most abstract form of information, is derived from individual processes of observation, measurement, or sensing. Data can be quantitative or qualitative but has minimal to no relational information or context. The binary encoding of information used by computers and the internet are excellent examples of data that is unintelligible until it is converted into information through the addition of context.

Information is less abstract and consists of data organized by relational context through processes of sorting, classifying, or indexing. This process of the relational grouping of data based on context is the most primitive form of intelligence. As such, the informational content of each data object is higher than pure data alone. Information paired with an intended receiver is called a message.

Knowledge exists in the thought-world of the observer as a theoretical description of a phenomenon under study.[19] It is a mental model of an observed phenomenon or interpretation of information.[20] Access to the phenomena or information about it is thus a requirement for knowledge creation. Knowledge is formed by cognition of the static and dynamic relationships of information informed by context, emotion, and exposure to past observations.[21] The accuracy of knowledge is probabilistic and must be continuously assessed against new observations to infer its relative validity, a measure of trust. Valid knowledge infers predictability of the observed phenomenon, presenting a kind of foresight.

Cognition, the conversion of information to knowledge, is continuous and occurs through conscious and unconscious reasoning, phenomena described by Daniel Kahneman's two-systems theory. System 1 thinking uses heuristics to quickly filter information and reach conclusions subconsciously and with minimal effort. System 2 is deliberate, conscious thinking that requires one's attention and effort and which produces some level of cognitive strain.[22] Although fast and less effortful, System 1 thinking is especially problematic as it actively filters information that does not fit one's preconceptions of reality, reducing one's likelihood of discovery and reinforcing preconceived notions.

Finally, cognition includes emotive factors and can answer questions about what one feels about what they think, and about what one knows about what they feel. As illusionists have known for centuries, the cognitive features of human biology can be hacked or tricked to induce people to reach perceptions in their thought-world that are entirely unsupported by reality.

Access, trust, and cognition are necessary for knowledge creation and are therefore fundamental to the information environment. This suggests a novel model for visualizing the information environment with knowledge as the emergent property of the integration of the fundamental elements (fig. 1).

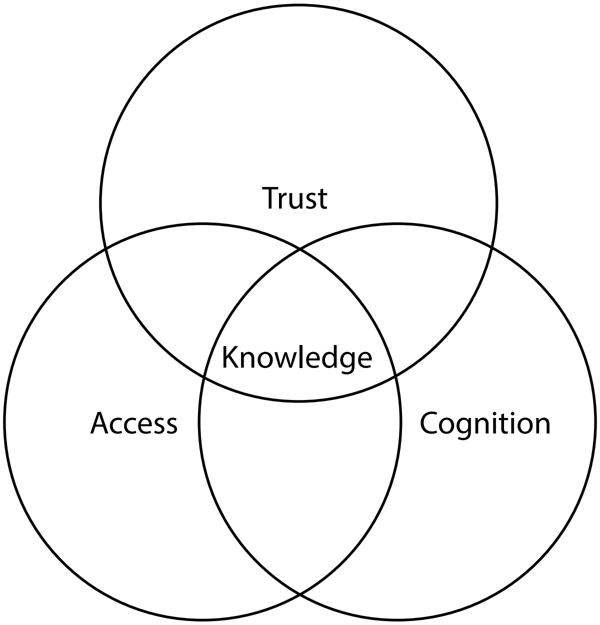


Figure 1. Fundamental elements of the information environment

Created by the author

This unique model defines the information environment using the fundamental elements of knowledge rather than defining it as a combination of "dimensions" paired with pre-existing military capabilities as is seen in Russian, Chinese, and American military conceptions.[23]

Data, information, and knowledge exist within a global super information ecosystem comprised of all the smaller information ecosystems, which may overlap or exist independent of one another. These information ecosystems are the physical and social information environments that people interact with and inhabit. The physical information ecosystems are the worlds people inhabit and can be directly and immediately observed. The social ecosystems extend people's perceptions to the broader world, well beyond their immediate environment, through social interactions and access enabled by means of communication such as writing and the internet. Fragmentation of information ecosystems occurs when access between ecosystems is reduced or does not exist.

It is important to emphasize that the preponderance of people's individual knowledge about the broader world is obtained through social interaction with others. This concept is often referred to as "the sociology of knowledge," where the individual's perceived reality, apart from that personally experienced, is "socially constructed."[24] In order to reduce uncertainty, the social construction of knowledge requires access to the social ecosystems of others, along with trust in the validity of shared information. Finally, the persistence of shared knowledge creates norms that can harden within people's mental models into heuristics that may or may not accurately fit one's continuously evolving environment, creating bias. The attributes of fragmentation, uncertainty, and bias comprise the first three problems of knowing.

Problems of Knowing

Three problems of knowing—fragmentation, uncertainty, and bias—emerge from the dysfunction or denial of the three fundamental elements of the information environment: access, trust, and cognition. Three additional problems emerge from vulnerabilities within the interplay of overlapping fundamental elements—root of trust, misinformation, and filtering. Combined, the six problems of knowing define the vulnerability space within the information environment model. As such, they are also described as attack vectors and are required for theorization about IW capabilities.

Fragmentation. As previously noted, information ecosystems are fragmented relative to other ecosystems when they have few or no connection paths between them. Fragmentation is categorized as physical, sociostructural, or voluntary. Physical fragmentation occurs as a consequence of the geographic separation of people groups. An instance of physical fragmentation resulting in surprise would be the "discovery" of the New World by Christopher Columbus. Similarly, the sight of a Western European was "new" to the indigenous North Americans as this knowledge was absent from their information ecosystem.

Sociostructural fragmentation occurs from efforts to control or deny information to others to preserve power hierarchies, worldviews, or paradigms. An example of this fragmentation is the trade guilds of the Middle Ages that sought to reduce trade competition through the preservation of specialized knowledge and craftsmanship. In today's information-centric society, sociostructural fragmentation includes the use of multilevel information security policies that preserve confidentiality through application of access controls.[25] Voluntary fragmentation occurs as an outward expression of rejecting unwanted information. Individuals may voluntarily attempt to avoid information from intruding into their ecosystems by deliberately cutting themselves off from it. Examples include ignoring or avoiding disturbing or degrading phenomena.

Filtering. Another problem of knowing emerges from the interaction between access to information and the heuristics that support cognition. Filtering occurs when a second party controls which information gets delivered to a person or when the information delivered to a person is ignored due to their heuristics. This problem is especially challenging because the information previously experienced by a person solidifies their heuristics. In turn, these heuristics can subconsciously filter out information that does not match preexisting mental models, a function of System 1 thinking also described as confirmation bias. Confirmation bias creates a reinforcement loop that continuously filters new information that does not match pre-existing bias until something occurs that does not match the preexisting mental model but that demands System 2's attention.

Uncertainty. A third problem of knowing is if and how much a person can trust the validity of information gleaned from others, which manifests itself as uncertainty. Since most knowledge comes from others instead of one's own personal observation and creation, trust is a measure of the validity of information received from others.[26]

Root of trust. A fourth problem of knowing, root of trust, exists within the interplay between the elements of access and trust and the problems of fragmentation and uncertainty. The root of trust problem extends directly to the discipline of information management where practitioners are concerned with the confidentiality, integrity, and availability of information. Among many threats, cybersecurity analysts concern themselves with preserving the integrity of data using check bit, hashing, and encryption algorithms to avoid data manipulation that could impact future information and knowledge. Of course, one must also trust the algorithms themselves are effective and have not been tampered with, and then one must also trust the hardware the algorithms use for their calculations, which means one must trust the hardware designers and manufacturers.

This multilayered trust hierarchy problem, often referred to as the "root of trust problem," was foreseen as far back as 1984 when computer science pioneer Ken Thompson published "Reflections on Trusting Trust."[27] The theoretical answer to ensuring high truth and low uncertainty requires the validity of information is not assumed if it was not personally created, and yet the overwhelming preponderance of information people continuously rely on comes from and is created by others. Human perceptions are based on trusting information from others who, in turn, base their perceptions on trusting information from others. As several security researchers have metaphorically described trust, "it's turtles, all the way down."[28]

Bias. A fifth problem of knowing, cognitive bias, is a consequence of how the human brain employs heuristics to interpret the environment while minimizing distractions and cognitive strain rapidly and efficiently. A heuristic is a cognitive shortcut that allows the subconscious, System 1, to reach a quick and reasonably accurate conclusion despite time constraints or limited information.[29] Some heuristics are innate to human nature while others are developed through repeated exposure to ideology, phenomena, or emotional events.[30] The problem of heuristics arises when the brain uses them to reach conclusions unsupported by reality. Further, when heuristics fail, the failures are unlikely to be detected until a significant event forces one's conscious thinking to recognize the mistake. This failure is called cognitive bias.

Social psychologist Jonathan Haidt identified especially powerful heuristics that are relevant to information warfare due to their strong ability to motivate individuals and groups. Haidt asserts there are "six psychological systems that comprise the universal foundations of the world's many moral matrices."[31] Each of his six moral psychological systems is labeled with value and antivalue pairs, where values are desired or accepted traits and antivalues are traits or actions that moral intuition rejects. These six foundations are care/harm, liberty/oppression, fairness/cheating, loyalty/betrayal, authority/subversion, and sanctity/degradation.

What makes this theory significant is that it provides a framework for understanding how moral biases influence global populations. In particular, the theory describes how groups use morality to motivate and order their societies according to social systems.[32] "Moral systems are interlocking sets of values, virtues, norms, practices, identities, institutions, technologies, and evolved psychological mechanisms that work together *to suppress or regulate self-interest and make cooperative societies possible* [emphasis added]."[33]

When it comes to power, the concept of a moral high ground is an appropriate metaphor since moral foundation biases shape how people interpret the world and motivate the actions they take within it, giving a moral positional advantage to some at the expense of others. These moral matrices shape people's biases and bind them into cooperative groups with shared values. At the same time, they blind people to the perspectives of others.[34]

This dynamic is important because if one understands the moral heuristics which drive a group of people, one can selectively present them with information that exploits and amplifies their naturally occurring potential for biased thinking and thus manipulate their behavior. In this way, bias can be weaponized to change behavior, potentially to violent extremes. Haidt's moral framework-based heuristics are just some of many heuristics that may exist within a population. Their relevance lies in their seemingly universal applicability to human behavior and potential for weaponization.

Misinformation. A sixth problem of knowing—misinformation—broadly captures subcategories of incorrect information, regardless of intent. When used to refer to a specific incident of false information, misinformation is generally assumed to be false information that is created or shared without the intent of causing harm. But when harm is intended, the subcategories of disinformation and malinformation are used. Disinformation "is an intentional spreading of misinformation in pursuit of a purpose-driven outcome."[35] Malinformation is data that reflects reality but is presented in a contextually misleading way.[36] In each case, the information is shared in the form of a message, manifesting itself in many different forms such as oral or written stories, images, and videos.

The proliferation of social media creates a global IW battleground in which, according to some researchers, "the defining feature is that messages are the munition."[37] These messages shape knowledge to align with or counter narratives—individual and shared stories people use to establish and reinforce mental models while making sense of perceived information. Finally, "propaganda" is misinformation used to "promote or publicize a particular political cause, ideological perspective, or agenda."[38]

Information Warfare Taxonomy

The elements of the IW theory outlined above are visualized beginning with the IW trinity, which positions individual and group perceptions of knowledge in the center of three overlapping rings of trust, access, and cognition (fig. 2). The six attack vectors of fragmentation—root of trust, uncertainty, misinformation, bias, and filtering—are shown as arrows pointing toward the IW elements that they exploit to create effects within the center. The resulting graphic depicts a taxonomy of IW.

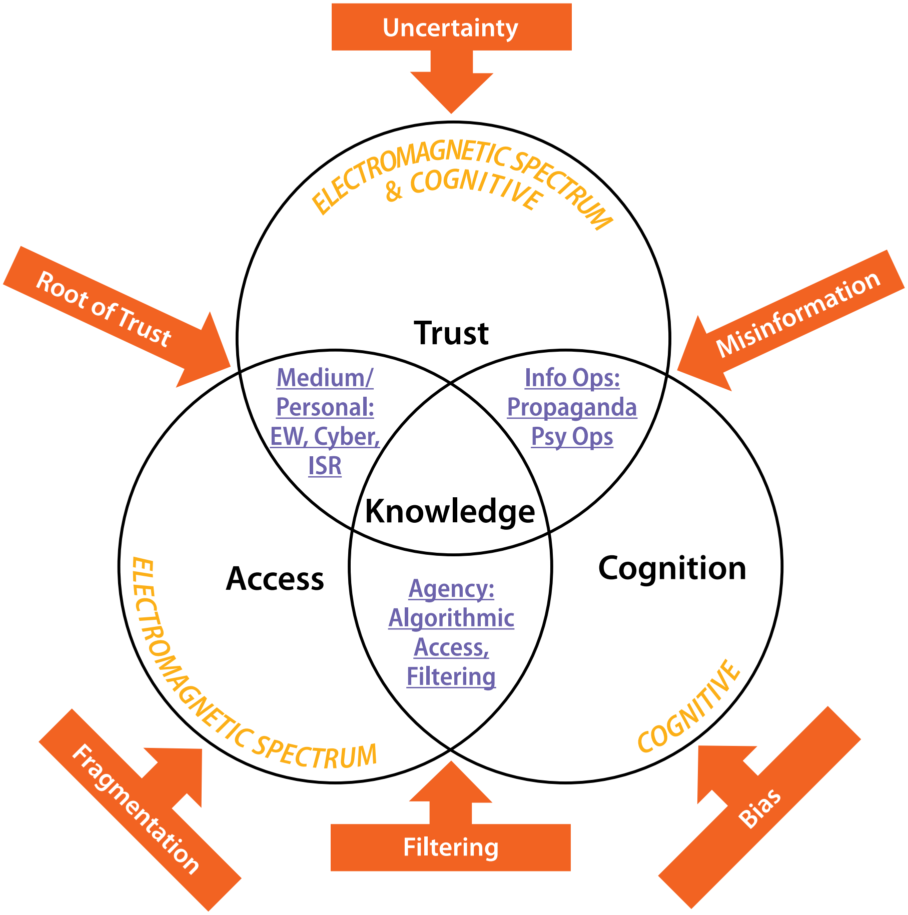

Uncertainty
ELECTROMAGNETIC SPECTRUM & COGNITIVE
Root of Trust
Misinformation
Trust
Medium/ Personal: EW, Cyber, ISR
Info Ops: Propaganda Psy Ops
Knowledge
Access
Cognition
Agency: Algorithmic Access, Filtering
ELECTROMAGNETIC SPECTRUM
COGNITIVE
Fragmentation
Filtering
Bias

Figure 2. Taxonomy of information warfare

Created by the author

The graphic posits three unique inferences. First, the information warfare environment is a blend of two domains, the cognitive domain imbued with trust and cognition, and the electromagnetic spectrum domain, which serves as the medium for information transfer and extends cognitive expressions of trust into the electromagnetic spectrum (in italics, fig. 2).

Second, three unique areas of overlap exist between each pair of rings that exclude the third ring. These areas possess unique characteristics and attack vectors. A nonexhaustive list of characteristics within each overlapping area is underlined for clarity. Finally, all three rings exist simultaneously. The character of each ring is continuously shaped by its relationship and interactions with the other two.

This taxonomy is a new way of conceptualizing IW based on its fundamental elements. These elements make up the IW trinity and reveal six IW attack vectors that exist across the full spectrum of information conflict. The result is a theoretical foundation that supports and informs a richer definition of IW.

Information Warfare Defined

Given this theoretical foundation, the article proposes the following working definition: Information warfare is the manipulation of knowledge through access, trust, and cognition to change the attitudes or behaviors of an individual or system. The aim of this definition is attitudinal or behavioral change, a concept not captured in a single English word, but one conceptualized within the Greek word *metanoia*, a "shift in mind" caused by new information or a new perspective and corresponding to a change in behavior.[39] Metanoia is the nature of IW.

This definition is supported by the three fundamental elements of the information environment—access, trust, and cognition. In contrast to the Air Force description, this definition allows capabilities to be developed across all instruments of power to achieve effects throughout the IW taxonomy, regardless of the level of competition. Notably, this definition accommodates current US military information warfare functions of cyberspace; intelligence, surveillance, and reconnaissance; electromagnetic warfare; electromagnetic spectrum management; and IO.

Simultaneously, this definition achieves overlap with the IW doctrine of America's competitors, such as Russia's *informatsionnaya voyna* (information war) functions of network operations, electronic warfare, psychological operations, and IO, and China's concept of "Informatized War," which privileges information advantage within the cyber, space, and electromagnetic domains.[40]

Crucially, the secondary regions of overlap reveal a conspicuous area of the triad not currently captured as a US doctrinal IO function or information-related capability. This space—the overlap of the fundamental elements of access and cognition—is where both physical and cognitive filtering mechanisms operate. This is significant because "the highest forms of communicative-based power in networked societies are the abilities to set the parameters for and guide the directional flow of discussions taking place within the network."[41] In this area of the triad, external filtering trains cognitive heuristics which, in turn, filter out information inconsistent with current mental models.

This suggests a role within IW for managing this battlespace that manipulates the relationship between fragmentation and bias and that can be heavily influenced by human-machine filtering such as machine-learning algorithms. In contrast with the United States, this is an IW function that US adversaries, particularly Russia and China, are already aggressively pursuing.

Theory of Victory

Like conventional warfare, the objective of IW is to achieve political objectives by coercing the enemy to do one's will.[42] But in contrast to the direct violence associated with conventional war, IW seeks to achieve its objective primarily by manipulating the fundamental elements of access, trust, and cognition.

Similarly, as the ultimate aim of conventional war is to disarm the enemy to impose one's will, the ultimate aim of IW is to disable the enemy's ability to use data, information, and knowledge to achieve its objective.[43] This aim is achieved when "the previous direction of messages [which inform and motivate] a political or military effect is . . . changed," thereby establishing a strategic, operational, or tactical information advantage.[44] China's theorists seem to agree, having stated in their 2013 *Science of Military Strategy* publication that information dominance is achieved when friendly forces can "seize and preserve the freedom and initiative to use information [while] simultaneously depriving an opponent" of the same.[45]

China's Information War

> *Most importantly, we must concentrate our efforts on bettering our own affairs, continually broadening our comprehensive national power, improving the lives of our people, building a socialism that is superior to capitalism, and laying the foundation for a future where we will win the initiative and have the dominant position.*
>
> Xi Jinping, speech to the Chinese Communist Party, January 5, 2013

The Chinese Communist Party (CCP) has clear, ambitious goals to solidify its long-term political control over China while securing increased global influence at the expense of the United States. According to the 2017 *US National Security Strategy*, China is first among nations competing with the United States for global influence as it seeks to "shape a world antithetical to US values and interests."[46]

The Biden administration considers China "the only competitor potentially able to mount a sustained challenge to a stable and open international system."[47] Most recently, Chinese media reported that President Xi Jinping considers the United States to be "the biggest source of chaos [and] the biggest threat to China's development and security."[48] China seeks to "displace the US in the Indo-Pacific region, expand the reaches of its state-driven economic model, and reorder the region in its favor."[49] Globally, China seeks to supplant the United States as the world's superpower while securing access to energy reserves and other vital national interests that will bolster China's continued growth.

After a perceived "century of humiliation," China sees itself as an ancient power, oppressed by foreigners but destined to return to preeminence as a regional hegemon. The CCP touts itself as "heir to a great civilization."[50] Led by Xi, the CCP seeks power through "Socialism with Chinese Characteristics," achieved through a narrative of China's rejuvenation.[51] The CCP seeks to fundamentally revise the world order and international norms in a way that places China in the center and serves the party's "authoritarian goals and hegemonic ambitions" through the establishment of a socialist international order.[52] The party intends to displace "the United States as the world's foremost power and restructure the world order to conform to the CCP's distinctive way of empire."[53] This is the objective of the China Dream, China's century-long unifying goal of restoring itself to preeminence by 2049.

China is an especially formidable IW adversary because the CCP believes it can "achieve its objectives through methods other than the use of brute military force."[54] With its propaganda-laden Marxist past, authoritarian present, and ambitious future, the IW trinity and attack vectors present an elegant way for China to achieve Sun Tzu's supreme art of war: "subdue the enemy's army without fighting at all."[55] This is especially true against an American adversary slow to confront the vulnerabilities inherent to the information environment relative to the Department of Defense and to the fundamental American values of freedom of speech and freedom of the press.

From its inception, the CCP used misinformation to achieve its political ends, considering thought management and propaganda against its own citizens to be the "lifeblood of the Party."[56] Mao Tse-tung, chairman of the CCP and founder of the People's Republic of China, overtly advocated for propaganda stating, "we should carry on constant propaganda among the people . . . so that they will build their confidence in victory."[57] The CCP organizes its misinformation efforts through many bureaucratic government organizations focused on its internal citizenry and on the populations of other countries. The United Front Work Department is one such organization and is responsible for "building support for the CCP and its policies among domestic ethnic groups, religious groups, the worldwide Chinese diaspora, and political, economic, and social elites in Hong Kong, Macao, and Taiwan."[58]

According to a 2019 Office of the Secretary of Defense report to Congress, "China conducts influence operations against media, cultural, business, academic, and policy communities of the United States, other countries, and international institutions to achieve outcomes favorable to its security and military strategy objectives . . . [the party] seeks to condition foreign and multilateral political establishments and public opinion to accept China's narrative."[59]

An example of this influence is the Ministry of Culture and Tourism that filters exposure to China's country and culture by arranging free and low-cost trips for journalists, politicians, sports stars, and other social influencers who might be willing to present a noncritical view of China when grassroots foreign support is needed.[60] Simultaneously, China denies access to individuals and corporations who portray China or the CCP in a negative light or who express sympathies contrary to China's interests.[61]

This aggressive filtering extends to China's printing industry that openly censors books printed within the country for export by demanding the removal of content that portrays China negatively or that does not align with its strategic goals.[62] Such censoring extends to the US sports and movie industries where threats to deny filming and lucrative distribution opportunities in China influence US production decisions while suppressing opinions counter to China's aims.[63] It is notable that Hollywood hasn't made a movie critical of China since 1997. Recently, China's National Film Administration directed the country's cinemas to show propaganda films a minimum of twice per week to commemorate the CCP's centennial anniversary.[64]

These efforts contribute to China's whole-of-government approach to achieving its national interests. To that end, China's Science of Military Strategy doctrine includes a section on "effective control," which describes the need to "energetically grasp military struggle while coordinating with political, economic, cultural, and diplomatic means under unified national deployment."[65] China's response to the COVID-19 pandemic provides a below-the-threshold-of-war example of how it applies the IW trinity and attack vectors to achieve effective control.

Under the CCP's guidance, China's informatized organizations used all means at their disposal to shape public opinion by controlling access to information, generating uncertainty about narratives that depicted China negatively, and appealing to the biases in each targeted population through misinformation.[66] China's filtering and fragmentation of information from health experts and journalists, its global delivery of misinformation narratives using social and mainstream media, and its efforts to generate uncertainty about the nature of the virus all demonstrate the aggressiveness and robustness of China's IW capabilities.[67]

Further, China seeks information advantage through hacking and other illegal access to advanced technologies and trade secrets from companies, universities, and the defense sectors of multiple nations. China's intellectual property theft has cost the United States approximately $250 billion per year over the past decade, with amounts in some years exceeding $600 billion. China's annual intellectual property theft approaches the US military's annual defense budget and exceeds the total profits of the top 50 US companies.[68] It has been called "the greatest transfer of wealth in history."[69]

The benefits to China include access to specialized knowledge, enabling it to pursue additional information advantages against governments, organizations, and persons across the globe.[70] Indeed, China's sustained efforts to gain access to the intellectual property of the breadth of US industry and defense contractors may compromise the root of trust of US hardware and software systems, generating uncertainty about the reliability of US networks and infrastructure. Finally, the scale of this intellectual property theft presents the possibility that China may have more information about US weapon system capabilities and vulnerabilities than that possessed by the US government.[71]

Finally, the CCP prepares its army to win Informatized Local Wars between information-based opponents.[72] Xi restructured the People's Liberation Army (PLA) in 2015, including standing up the Strategic Support Force which conducts many aspects of IW, including intelligence, technical reconnaissance, cyberespionage, cyberattack, cyberdefense, electronic warfare, and aspects of information technology and management.[73]

Some researchers claim when Xi speaks of a "fully modernized force in 2035," he "no doubt envisions a PLA capable of conducting joint informatized operations in the context of systems-destruction warfare, giving the CCP a tool to achieve political objectives while controlling the scope and scale of conflict."[74] The PLA sees the information domain as "first and foremost in importance." It treats information dominance in the form of controlled and persistent access within the cyber, space, and electromagnetic spectrum domains early in a conflict as a pretext for achieving victory, while seeking to fragment or otherwise deny the same to its enemies.[75]

China has a robust IW capability honed from decades of IO performed against its domestic population and overseas adversaries. It is adept at using all elements of IW to achieve information advantage. This information advantage supports every Chinese national interest, and every national interest serves to reinforce the legitimacy and stability of the authoritarian CCP regime.

Recommendation

> *Our open economies and open societies have allowed the CCP to have an undue influence on our public sphere. . . . It will take recognition of this influence and a major strategic adjustment to correct this.*
>
> Anne-Marie Brady, "China Wants Face and We Are Left with the Cost"

A recently declassified intelligence report determined the United States "has not sufficiently adapted to a changing geopolitical and technological environment increasingly shaped by a rising China and the growing importance of interlocking non-military transnational threats. . . . Absent a significant realignment of resources, the U.S. government . . . will fail to achieve the outcomes required to enable continued U.S. competition with China on the global stage for decades to come, and to protect the U.S. health and security."[76] The United States is unable to effectively compete within the information environment due to a "lack of bureaucratic coherence and leadership."[77] Meanwhile, every American is vulnerable to information warfare as an unwitting victim within the information environment.[78]

To reverse this trend, the United States must define information warfare in a way that empowers a doctrinal framework for thinking, communicating, planning, and acting within the information environment while organizing to meet the threat.

This article presents a novel theory of IW constructed using first principles of information theory to create a comprehensive IW taxonomy that includes the IW trinity of access, trust, and cognition, along with six IW attack vectors. This taxonomy provides a solid foundation for conceptualizing information warfare and informs how the United States defends itself while pursuing national interests within the information environment. This theory should be extended to create robust IW doctrine that elaborates upon the full IW taxonomy.

Conclusion

> *These events were not the products of ineluctable forces outside the boundaries of human choice; they were the results of decisions and actions by people who had opportunities to choose and act otherwise.*
>
> D. H. Fischer, *Washington's Crossing*

Shortly after Russia used information warfare to tarnish the American election process in 2019, the CCP proved the profound danger it presents to itself and to the world in its deliberate mishandling of COVID-19.[79] The same "you die, I live" worldview is using IW to pursue information advantage in artificial intelligence, quantum computing, robotics and automation, space, oceanic engineering, biotechnology, advanced pharmaceuticals, and next-generation energy and power generation. Both countries continue to use IW to directly support their national interests while damaging and discrediting their global competitors, including the United States.[80]

The lessons from the Battle of Megiddo apply today as they did 3,500 years ago. The focus and capacity of America's instruments of power stand divided between competing with China and Russia militarily and economically. These are the two roads on which the United States expects their approach. The IW fight is America's third road, and it leads deep into the nation, directly to the hearts and minds of its citizens—the US government's center of gravity. The United States must orient itself to counter how China and Russia are choosing to fight—information warfare. We ignore it at our peril. ✪

Daniel Morabito

Lieutenant Colonel Daniel "Plato" Morabito, commander of the 834th Cyberspace Operations Squadron, 67th Cyberspace Wing, Joint Base San Antonio, Texas, holds a master of science in leadership and information technology from Duquesne University, a master of science in cyberspace operations from the Air Force Institute of Technology, a master of military operational art and science from the USAF Air Command and Staff College, and a master of arts in military operations from the US Army Command and General Staff College.

Notes

[1] Richard Dupuy and Trevor Dupuy, *The Encyclopedia of Military History: From 3500 BC to the Present* (New York: Harper and Row, 1970), 5.

[2] Eric H. Cline, *The Battles of Armageddon: Megiddo and the Jezreel Valley from the Bronze Age to the Nuclear Age* (Ann Arbor, MI: University of Michigan Press, 2002), 18–19.

[3] Harold Hayden Nelson, *The Battle of Megiddo* (Chicago: University of Chicago Press, 1913), 38.

[4] Nelson, *The Battle of Megiddo*, 22–38.

[5] Dupuy and Dupuy, *Encyclopedia of Military History*, 6.

[6] Jeffrey M. Reilly, *Operational Design: Distilling Clarity from Complexity* (Maxwell AFB, AL: Air Force Research Institute, 2012), 21–23.

[7] James J. Schneider, *Vulcan's Anvil: The American Civil War and the Emergence of Operational Art,* Theoretical Paper No. 4 (Fort Leavenworth, KS: School of Advanced Military Studies, 1995), 10–11.

[8] Sara Kitsch et al., *Quick Look: Inoculation Theory*, (Stillwater: The Media Ecology and Strategic Analysis Group (MESA), School of Media and Strategic Communications, Oklahoma State University, November 2020), https://nsiteam.com/.

[9] Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 25, https://www.acq.osd.mil/.

[10] Edward Waltz, *Information Warfare Principles and Operations* (Boston: Artech House, 1998), 19–30.

[11] Office of the Joint Chiefs of Staff (CJCS), *Competition Continuum,* Joint Doctrine Note 1-19 (Washington, DC: CJCS, 2019), 2-4; and Bradley Young and Jonathan Wood, "The Army's Information Operations Profession Has an Identity Crisis," *Proceedings* 147, no. 3 (March 2021), https://www.usni.org/.

[12] CJCS, *Information Operations,* Joint Publication (JP) 3-13 (Washington, DC: CJCS, 2014), GL-3.

[13] US Department of the Air Force (DAF), "Sixteenth Air Force (Air Forces Cyber)," DAF (website), August 27, 2020, https://www.16af.af.mil/; and CJCS, JP 3-13, ix.

[14] John Boyd, *A Discourse on Winning and Losing* (Maxwell AFB, AL: Air University Press, 2018), 237; and Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 75.

[15] CJCS, *Joint Planning,* JP 5-0 (Washington, DC: CJCS, 2020).

[16] CJCS, JP 5-0, II-10, III-33.

[17] Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington, VA: Center for Naval Analysis, 2016), 3; and Edmund Burke et al., *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 6–8, https://www.rand.org/.

18. Iain King, "Toward an Information Warfare Theory of Victory," Modern War Institute, October 19, 2020, https://mwi.usma.edu/.

19. Susan J. Milton and Jesse C. Arnold, *Introduction to Probability and Statistics: Principles and Applications for Engineering and the Computing Sciences* (New York: Tata McGraw-Hill, 2007), 1.

20. Venkatesh Rao, *Tempo: Timing, Tactics and Strategy in Narrative Decision-Making* (La Vergne, TN: Ribbonfarm, 2011), 42.

21. Waltz, *Information Warfare*, 83–85.

22. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Allen Lane, 2011), 21–24.

23. Bryan Clark, Daniel Patt, and Harrison Schramm, *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations* (Washington, DC: Center for Strategic and Budgetary Assessments, February 11, 2020), 22; and CJCS, JP 3-13, I-1–I-3.

24. Peter Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (New York: Anchor Books, 1967), 3.

25. Matt Bishop, *Computer Security: Art and Science* (Upper Saddle River, NJ: Addison-Wesley, 2002), 124.

26. Berger and Luckmann, *Social Construction*, 61.

27. Ken Thompson, "Reflections on Trusting Trust," *Communications of the ACM* 27, no. 8 (August 1984): 763, https://www.cs.cmu.edu/.

28. Jonathan M. McCune et al., "Turtles All the Way Down: Research Challenges in User-Based Attestation" (paper presented at 2nd USENIX Workshop on Hot Topics in Security, Boston, MA, August 2007), https://www.usenix.org/.

29. Michael Janser, *Cognitive Biases in Military Decision Making* (Carlisle Barracks, PA: US Army War College, 2007), 1, https://apps.dtic.mil/.

30. Jonathan Haidt, *The Righteous Mind: Why Good People Are Divided by Politics and Religion* (New York: Vintage, 2012), 153.

31. Haidt, *Righteous Mind*, 211.

32. Haidt, *Righteous Mind*, 16–17.

33. Haidt, *Righteous Mind*, 314.

34. Haidt, *Righteous Mind*, 221–22.

35. Zachery Kluver et al., *Propaganda: Indexing and Framing the Tools of Disinformation*, Quick Look (Stillwater: MESA, School of Media and Strategic Communications, Oklahoma State University, December 2020), 3, https://nsiteam.com/.

36. Claire Wardle and Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe (CoE) Report DGI (Strasbourg, France: CoE, September 27, 2017), 20, https://rm.coe.int/.

37. King, "Theory of Victory," 4.

38. Kluver et al., *Propaganda*, 1.

39. Peter M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization,* rev. ed. (New York: Currency, 2006), 13–14.

40. Connell and Vogler, *Cyber Warfare*, 3; and Burke et al., *Operational Concepts*, 6-8.

41. Kluver et al., *Propaganda*, 1.

42. Clausewitz, *On War*, 75.

43. Clausewitz, *On War*, 77.

44. King, "Theory of Victory," 5; and Timothy D. Haugh, Nicholas J. Hall, and Eugene H. Fan, "16th Air Force and Convergence for the Information War," *Cyber Defense Review* 5, no. 2 (Summer 2020): 29, https://www.jstor.org/.

45. Xiaosong Shou, ed., *The Science of Military Strategy* (Beijing: Military Science Press, 2013), 245.

46. Trump, *National Security Strategy*, 25.

47. Joseph R. Biden Jr., *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), 8, https://www.whitehouse.gov/.

48. Yuying Ma, "He Bin Made a Speech at a Seminar on the Study and Implementation of the Fifth Plenary Session of the 19th Central Committee of the Communist Party of China at the County Level," *Qilian News*, February 25, 2021, https://web.archive.org/.

49. Trump, *National Security Strategy*, 25.

50. Policy Planning Staff, Office of the Secretary of State, *The Elements of the China Challenge* (Washington, DC: US Department of State, December 2020), 6, https://www.state.gov/.

51. Michael A. Peters, "The Chinese Dream: Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era," *Educational Philosophy and Theory* 49, no. 14 (November 2017): 1299–1304, https://doi.org/.

52. Policy Planning Staff, *China Challenge,* 1.

53. Policy Planning Staff, *China Challenge*, 7.

54. Dennis J. Blasko, "Special: Sun Tzu Simplified: An Approach to Analyzing China's Regional Military Strategies," Project 2049 Institute, April 10, 2015, https://project2049.net/.

55. Roger T. Ames, *Sun-Tzu: The Art of Warfare: The First English Translation Incorporating the Recently Discovered Yin-ch'ueh-shan Texts* (New York: Ballantine Books, 2010), 111.

56. Anne-Marie Brady, *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China* (Lanham, MD: Rowman and Littlefield, 2009), 1.

57. Mao Tse-tung, "On the Chungking Negotiations," in *Selected Works of Mao Tse-tung*, vol. 4, October 17, 1945, 59–60, https://www.marxists.org/.

58. Larry Diamond and Orville Schell, eds., *Chinese Influence and American Interests: Promoting Constructive Vigilance* (Stanford, CA: The Hoover Institution, 2018), 138, https://www.hoover.org/.

59. Office of the Secretary of Defense (OSD), *Annual Report To Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC: OSD, May 2, 2019), i, https://media.defense.gov/.

60. Anne-Marie Brady, "Magic Weapons: China's Political Influence Activities under Xi Jinping" (paper presented at the Taiwan Foundation for Democracy Conference, Arlington, VA, September 16–17, 2017), https://www.wilsoncenter.org/.

61. Sitong Guo et al., "The Tweet Heard Round the World: Daryl Morey, the NBA, China, and Attribution of Responsibility," *Communication & Sport* (December 2020), https://doi.org/.

62. Harrison Christian, "Kiwi Publishers Face Censorship Demands from Chinese Printers," Stuff, August 18, 2019, https://www.stuff.co.nz/; and Sarah Wu and Joyce Zhou, "Editing History: Hong Kong Publishers Self-Censor under New Security Law," Reuters, July 13, 2020, https://www.reuters.com/.

63. Victor Cha and Andy Lim, "Flagrant Foul: China's Predatory Liberalism and the NBA," *Washington Quarterly* 42, no. 4 (December 2019): 23–42, https://doi.org/; and Ben Cohen, "LeBron James Says Tweet Supporting Hong Kong Protests Was 'Misinformed,'" *Wall Street Journal*, October 14, 2019, https://www.wsj.com/.

64. Anne-Marie Brady, "China Wants Face and We Are Left with the Cost," commentary (Ottawa, Ontario: Macdonald-Laurier Institute, March 2020), 1, https://www.macdonaldlaurier.ca/; and Rebecca Davis, "China's Film Authority Orders All Cinemas to Screen Propaganda Films at Least Twice a Week," *Variety,* April 2, 2021, https://variety.com/.

65. Xiaosong, *Military Strategy*, 112.

66. Eric Chan and Peter Loftus, "Chinese Communist Party Information Warfare. US-China Competition during the COVID-19 Pandemic," *Journal of Indo-Pacific Affairs* (Summer 2020): 146–54, https://media.defense.gov/.

67. Chan and Loftus, "Information Warfare," 146–54.

68. Policy Planning Staff, *China Challenge*, 10.

69. Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" *Foreign Policy*, July 9, 2012, https://foreignpolicy.com/.

70. Policy Planning Staff, *China Challenge*, 6–7.

71. Shannon Vavra, "NSA Warns Defense Contractors of Recent Chinese Government-backed Hacking," Cyberscoop, October 20, 2020, https://www.cyberscoop.com/.

72. Burke et al., *Operational Concepts*, 7.

73. Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* 3, no. 1 (Spring 2018): 111–15, https://cyberdefensereview.army.mil/.

74. Burke et al., *Operational Concepts*, 6.

75. Burke et al., *Operational Concepts*, 7.

76. House Permanent Select Committee on Intelligence (HPSCI), *The China Deep Dive: A Report on the Intelligence Community's Capabilities and Competencies with Respect to the People's Republic of China*, redacted unclassified summary (Washington, DC: United States House of Representatives, September 30, 2020), 8, https://intelligence.house.gov/.

77. James Micciche, "U.S. below War Threshold Options against China," Divergent Options, September 21, 2020, https://divergentoptions.org/.

78. Scott Padgett and Stefan Banach, "Winning the Real War: Designing Virtual Armies," Small Wars Journal, April 9, 2019, 2021, https://smallwarsjournal.com/.

79. HPSCI, *China Deep Dive*, 3.

80. Policy Planning Staff, *China Challenge*, 13, 33.

STRATEGIC COMPETITION

Combatting Russian Influence through Improved Security Assistance

Walter Richter

When a partner nation undertakes major military modernization efforts through the vehicle of foreign military sales (FMS), especially in aircraft, the process often takes four to five years from the initial request until delivery.[1] As a result, many countries extend or even establish new contractual agreements with Russian manufacturers to maintain Soviet-legacy defense systems in order to preserve their national defense capabilities. The paradoxical effect is that countries transitioning from Russian-produced to US-produced defense systems often fall under even greater Russian influence during this period.

The United States can counter this influence through security assistance mechanisms such as leveraging existing Allied and partner maintenance capabilities, working with existing US partnership efforts, and improving the FMS total package approach.

Confronting Russian Influence

The United States' 2021 *Interim National Security Strategic Guidance* identifies Russia as a competitor "determined to enhance its global influence and play a disruptive role on the world stage."[2] This recognition comes after Russia has violated borders in attempts to dominate the economic, diplomatic, and security decisions of its neighboring states.[3] As the world's second-largest arms exporter, Russia exerts significant influence by controlling the maintenance certification of Soviet-legacy defense systems that many countries still use nearly 30 years after the collapse of the Soviet Union.[4]

In response, the United States has leveraged its security assistance with programs such as the European Recapitalization Initiative Program, designed to bolster Allies and partners facing Russia's revisionist aggression.[5] Programs such as this use foreign military finance grants to enhance capabilities and NATO interoperability through FMS.[6] Also, restrictive efforts such as the 2017 Countering America's Adversaries Through Sanctions Act (CAATSA) seek to reduce Russian influence by sanctioning governments and persons who facilitate significant transactions for or on behalf of Russia.[7]

Maintaining Legacy Systems

After their decisions to purchase US-produced military aircraft, Slovakia and Bulgaria had to continue agreements with Russian manufacturers to maintain their Soviet-legacy systems until the US systems were delivered.[8] Slovakia faced this crisis with both rotary- and fixed-wing aircraft. After agreeing to purchase nine UH-60M Blackhawk helicopters in 2015, Slovakia waited five years for full aircraft delivery and chose to maintain its existing Mi-17 helicopters in the interim, which led to further agreements with Russia.[9] While Slovakia could maintain its Mi-17 helicopters, Russia controlled the maintenance certification of those aircraft. Slovakia faced a similar situation in 2018 when it agreed to purchase F-16 Block 70 aircraft through FMS: in the period between purchase and acquisition, it had to continue to maintain its MiG-29 aircraft inventory.[10]

This scenario repeated itself in 2019 when Bulgaria agreed to purchase F-16 aircraft through FMS but also sought to maintain its MiG-29 aircraft,[11] which risked violating CAATSA. Today Croatia is facing a similar dilemma as it seeks to purchase US-produced aircraft but requires interim maintenance for its MiG-21 aircraft.[12]

Letting Legacy Systems Fail

As the United States promotes NATO-interoperable solutions through either FMS, third-party transfers, or direct commercial sales, it should consider solutions to support the transition from Soviet-legacy equipment.[13] While the FMS total package approach includes training and maintenance support, it does not specifically support the transition away from a legacy system. This omission can leave countries with the choice of letting maintenance certificates expire, ignoring CAATSA to extend agreements with Russia, or seeking alternative maintenance certification during their modernization transition period.

Allowing maintenance certificates to expire generally results in a loss of military airworthiness certification from the European Defence Agency. Nations that lose this certification may experience a degradation in air-policing capabilities with an inability to conduct cross-border operations.[14] Albania, Montenegro, and Slovenia have allowed maintenance certificates to expire but now receive air policing from the Italian, Greek, and Hungarian Air Forces.[15] Similarly, NATO Allies provide air-policing support to the Baltic states of Estonia, Latvia, and Lithuania. While these efforts secure Alliance airspace and promote cooperation among NATO members, the United States should work to create more capabilities among partners and Allies, not greater requirements.

Slovakia and Bulgaria have chosen to ignore CAATSA and cooperate with Russia to maintain legacy systems. Beyond the problem of Russian influence, this cooperation often places Russian technicians near newly arriving NATO aircraft, endangering the proprietary and classified nature of the technology. Violations of CAATSA lessen the benefit of adopting NATO-interoperable aircraft, placing smaller countries into difficult negotiations with Russia and potentially damaging their relationships with the United States.

Leveraging Existing In-Country Capabilities

Ironically, many of these countries can already perform work on legacy fixed- and rotary-wing Russian aircraft at their maintenance, repair, and overhaul (MRO) facilities. Such facilities exist in Bulgaria, Czechia, Lithuania, Poland, Romania, and Slovakia.[16] Unfortunately, maintenance certification still resides with Russian manufacturers who can withhold certification for customers transitioning away from Russian defense systems.

In the case referred to above, Bulgaria initially intended to use Poland's MRO facility at Bydgoszcz, which maintains MiG-29 aircraft without Russian certification. But legal threats from Russia led Bulgaria to determine the Russian manufacturer was the only reliable option.[17] As a result, Bulgaria signed a $51 million contract with the manufacturer to modernize its MiG-29 aircraft.[18] Since then, Bulgaria has signed additional maintenance contracts with the manufacturer to sustain its NATO air-policing mission, despite operating its facility in Plovdiv, capable of maintaining MiG-29 aircraft.[19]

In Slovakia, the *Letecké Opravovne Trenčín* aircraft maintenance facility continues to maintain and overhaul Russian Mi-17 helicopters despite their Russian maintenance certification expiring, most notably under contract to the NATO Security and Procurement Agency for Afghan Air Force Mi-17 helicopters.[20] While some European countries will not accept Russian aircraft maintenance certification from any facility not certified by Russia, Poland's willingness to certify maintenance on their MiG aircraft and at least offer that service to Bulgaria, as well as Slovakia's work for NATO on Afghan Air Force Mi-17 helicopters, help weaken Russian influence.

Leveraging Existing DOD Partnerships

Another option to confront a country's dependence upon Russia for aircraft maintenance is providing access to US-produced aircraft by loaning aircraft or providing flying hours with a partnered USAF fixed-wing or US Army rotary-wing unit.

The US National Guard State Partnership Program, which partners 21 Air and Army National Guards with 22 countries in the United States European Command area of responsibility, already supports combined aviation operations and exercises between countries and partnered states and could be an official element of FMS.[21] Additionally, active and reserve Army and Air Force units conducting force rotations in Europe, such as the USAF 457th Expeditionary Fighter Squadron, which is in Romania and is flying with the Romanian Air Force, could support countries awaiting delivery of US aircraft through FMS.[22]

Rethinking the Total Package Approach

The FMS goal to provide capabilities to a partner or an Ally through a total package approach has made FMS a popular choice for many countries. In order to increase that competitive advantage, the Department of Defense should consider a plan to guide a country, not just from initial request to full fielding but through its transition away from Soviet-legacy systems with a combination of the aforementioned methods. Such a plan could significantly enhance the military capabilities of Allies and partners and help achieve the objectives of FMS to "strengthen the security of the U.S. and promote world peace."[23]

Assisting Ally and partner militaries' transition toward NATO interoperability will require multiple solutions. Despite the legal and logistical challenges, MRO support could be effective in reducing a country's dependence on Russia for Soviet-legacy aircraft maintenance. Although limited spare parts and potential legal challenges by countries not accepting alternative maintenance certificates make this approach problematic, it could be part of a range of solutions for an Ally or partner military to maintain rotary- or fixed-wing aviation capabilities.

When MRO support is not an option, Ally and partner access to US aircraft through the National Guard's State Partnership Program or through cooperation with rotating US Army or USAF units could enable earlier adoption of NATO interoperable solutions and limit Russian influence. Furthermore, cooperation, either with rotating USAF units or through the State Partnership Program, enhances the abilities of US, Ally, and partner pilots, builds relationships that promote better interoperability, and could assist US efforts toward access, basing, and overflight.

Conclusion

Foreign military sales, which provide access to the latest US technology with training and maintenance support, continue to attract Ally and partner countries. But if the United States wants to be competitive, it should support necessary supplier transition periods as well. Despite the challenges, facilitating these transition efforts could better enable Ally and partner militaries to achieve greater interoperability, reduce Russian influence, and ultimately build closer working relationships with the United States. Supporting transition efforts could be the difference for many countries between enhancing NATO capabilities or remaining within Russia's logistical sphere of influence. Our European Allies and partners are standing at a crossroads and are looking to the United States for leadership. We should not waste this opportunity. ✪

Walter Richter

Colonel Walter Richter, USA, holds a master of operational studies from the US Marine Corps School of Advanced Warfighting, a master of strategic studies from US Army Command and General Staff College, and is the US Army attaché at the US Embassy in Berlin, Germany.

Notes

[1] Estimate based on the author's experience as a chief of defense cooperation in a former Warsaw Pact state and overseeing US European Command's security cooperation efforts in the states of former Yugoslavia.

[2] Joseph R. Biden Jr., *Interim National Security Strategic Guidance* (Washington, DC: White House, March 2021), https://www.whitehouse.gov/, 8.

[3] James N. Mattis, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Office of the Secretary of Defense, January 2018), https://dod.defense.gov/, 1.

[4] Vusala Abbasova, "*Russia Remains World's Second Largest Exporter: Report*," Caspian News, March 19, 2021, https://caspiannews.com/.

[5] Christopher A. Ford, *Security Assistance and U.S. Competitive Strategy: Improving Our Game*, Arms Control and International Security Papers 1, no. 3 (Washington, DC: Office of the Under Secretary of State for Arms Control and International Security, April 21, 2020): 3, https://www.state.gov/.

[6] Ford, *Security Assistance*, 4.

[7] Congressional Research Service (CRS), *U.S. Sanctions on Russia: An Overview*, In Focus (Washington, DC: CRS, June 7, 2021), https://fas.org/.

[8] "Slovakia to Sign €100 Million Contract with Russia for Servicing MiG-29 Fleet," Military Watch, June 6, 2019, https://militarywatchmagazine.com/; "Bulgarian Government Approves 183M Leva Projects to Overhaul MiG-29, Su-25 Combat Aircraft," Sophia Globe, November 28, 2018, https://sofiaglobe.com/; and Irina Dzamic, "Scandal with Ukrainian MiGs in Croatia" LB.ua, February 11, 2018, https://en.lb.ua/.

[9] Jakub Groszkowski, "Prime Minister Fico's Russian Card," Osrodek Studiów Wschodnich (Centre for Eastern Studies), July 1, 2015, https://www.osw.waw.pl/.

[10] Krassimir Grozev and Alexander Mladenov, "Total Renewal," AIR International, September 28, 2017, https://www.airinternational.com/.

[11] "Bulgaria Gives Final Green Light to Biggest Military Acquisition since Fall of Communism," RadioFree Europe/Radio Liberty, July 31, 2019, https://www.rferl.org/; and "Bulgaria

Allocates 16M Leva for MiG-29 Fighter Jets Overhaul," Sophia Globe, December 4, 2019, https://sofiaglobe.com/.

12. Garrett Reim, "How Lockheed Martin Plans to Speed Up Sales with Commoditised F-16," Flight Global, September 4, 2020, https://www.flightglobal.com/; and "Croatia Intensifies MiG-21 Replacement Efforts," Air Recognition, January 16, 2020, https://airrecognition.com/.

13. Office of the Deputy Assistant Secretary of the Army for Defense Exports and Cooperation (DASA/DE&C), "Security Assistance," DASA/DE&C (website) accessed April 1, 2021, https://www.dasadec.army.mil/.

14. "Military Airworthiness," European Defence Agency (website) accessed April 1, 2021, https://www.eda.europa.eu/.

15. "Air Policing over the Western Balkans," NATO (website), accessed April 1, 2021, https://ac.nato.int/.

16. "History," Avionams Aircraft Repair Plant (website), accessed April 2021, http://www.avionams.com/; "LOM Praha," company information, LOM Praha, (website), accessed April 2021, https://www.lompraha.cz/; "Lithuanian Company to Help Maintain Ethiopian Air Force Aircraft," DefenceWeb, March 22, 2016, https://www.defenceweb.co.za/; Andrzej Hladij, "New Capabilities at Hand of the Polish Military Aviation Works Facility in Bydgoszcz. Support for the Hercules Transport Aircraft and Airliners," Defence 24, September 30, 2016, https://www.defence24.com/; Marino Boric, "Aerostar's Road to a Better Future," AviationPros, June 26, 2019, https://www.aviationpros.com/; and "Aviation Platforms," Letecké Opravovne Trenčín (website), accessed July 13, 2021, https://lotn.sk/.

17. Jaroslaw Adamowski, "Russia's MiG Warns Bulgaria over Jet Deal with Poland," DefenseNews, October 2, 2015, https://www.defensenews.com/.

18. "NATO Member Bulgaria Contracts Russian Assistance to Maintain Fighter Jets," Military Watch, March 22, 2018, https://militarywatchmagazine.com/.

19. Aleksia Petrovia, "Bulgaria Signs Deal for Maintenance of 10 Engines for MiG-29 Jets," SeeNews, January 7, 2020, https://seenews.com/; and Avionams Aircraft Repair Plant, "History."

20. "Russia Accuses Slovakia of Illegally Repairing Afghanistan's Mi-17 Helicopters," Defense World, March 18, 2019, https://www.defenseworld.net/.

21. US Department of Defense, National Guard Bureau, "The State Partnership Program (SPP)," powerpoint presentation, June 2020, https://www.nationalguard.mil/.

22. Dylan Malyasov, "U.S. F-16 Fighting Falcons to Take Part in Joint Exercises with Romanian MiG-21 Fighters," Defence Blog, May 11, 2019, https://defence-blog.com/.

23. "Foreign Military Sales (FMS)," Defense Security Cooperation Agency (website), accessed April 2021, https://www.dsca.mil/.

TECHNOLOGY

Shifting Satellite Control Paradigms

Operational Cybersecurity in the Age of Megaconstellations

CARL POOLE
ROBERT BETTINGER
MARK REITH

The introduction of automated satellite control systems into a space-mission environment historically dominated by human-in-the-loop operations will require a more focused understanding of cybersecurity measures to ensure space system safety and security. On the ground-segment side of satellite control, the debut of privately owned communication antennas for rent and a move to cloud-based operations or mission centers will bring new requirements for cyber protection for both Department of Defense (DOD) and commercial satellite operations alike. It is no longer a matter of whether automation will be introduced to satellite operations, but how quickly satellite operators can adapt to the onset of control automation and promote cybersecurity in an increasingly competitive, contested, and congested space domain.

Introduction

Control automation has spread from industrial manufacturing and self-driving cars to home and household appliances. Control automation has also moved into the realm of satellite-control operations, with the focus of satellite-control automation being driven on two fronts. First, the ability to incorporate cost-effective, highly capable equipment in the satellite design allows for an increase in onboard controls processing. Second, the proliferation of space operations in various orbital regimes—this article will focus on low-Earth orbit (LEO)—is pushing complex tasks, such as satellite-link scheduling and conjunction-avoidance maneuvers, beyond the control of human operators.

An additional operational distinction is made between satellite automation—the self-contained system process of conducting repetitive tasks—and satellite autonomy, which gives the satellite the ability to implement changes with limited to no human-in-the-loop actions.[1] This distinction will add a level of complexity to the cybersecurity of satellite control. Placing tasks previously controlled by humans under the control of a computer-executed algorithm may be the only viable way to manage the development of future megaconstellations and enable effective space-traffic management.[2] But the prospect of improved space-traffic safety and collision avoidance via control automation raises several concerns.

While increasing the levels at which LEO constellations can interact and cooperate, the needed hardware infrastructure and data-exchange alterations that will allow for such interoperability will introduce new entry points that, in turn, will likely increase cybersecurity risks. The introduction of software-defined equipment, cloud-based mission-control centers, and Ground Stations as a Service (GSaaS) are prime examples. Space and cybersecurity professionals will need increased interactive cooperation and mission understanding to address new potential cybersecurity issues presented by emerging commercial space applications and automation.

Current Satellite Control Operations

The control architecture for satellites has remained nearly constant since the beginning of the Space Age in the mid-twentieth century. Starting with the launch of the first artificial satellites, each on-orbit system has mostly featured a unique design, function, and mode of operation. This uniqueness has led to self-contained and independent operating procedures controlled by the satellite owner. In the typical satellite-control structure, a satellite downlinks information such as payload data and spacecraft state-of-health information when it is within view of a ground-based receiver. From the receiver, the information is processed and passed to the satellite operations center (SOC), which reviews it for faults and assesses the need for required operating adjustments and/or new system instructions.

In the case of orbital maneuvers to correct for position or to change location (such as slewing, station keeping, or collision avoidance with another object), one member of the operations team scripts the commands for the prescribed maneuver. Several operations team members then review the script before passing it to the human-in-the-loop satellite operator for processing. During the next scheduled uplink opportunity with the satellite, the commands are sent from the SOC to the transceiver and then to the satellite for processing and command execution. This type of hands-on approach developed due to constraints in the onboard systems, specifically, limited computing power and proprietary operating structures.

The emphasis on human control ostensibly meant reduced concerns for cybersecurity and an increased sense of command situational awareness due to the human use of protected ground communications systems and owner-controlled data links. Despite its benefits, this process can be very time-consuming, and task scheduling becomes increasingly complex with the addition of new satellites to the satellite-control architecture. Consequently, this human-in-the-loop satellite-control architecture will be unable, without a substantial increase in infrastructure, manning, and funding, to effectively manage the size of megaconstellations of the near future.

Anatomy of Megaconstellations

The development of constellations consisting of thousands of individual satellites controlled by one operator is no longer a wistful dream of science fiction or avant-garde technologists. With the introduction of LEO constellations such as "Starlink" or "OneWeb," the concept of megaconstellations is becoming a reality, precipitating the rise of megaconstellations as a potential means to provide regional and global telecommunications services.[3]

In Asia, China Telecom reportedly plans to create a 10,000-satellite megaconstellation called "China StarNet" in the next 5–10 years.[4] In late 2020, the European Union revealed plans to initiate a program to develop a telecommunications megaconstellation to establish "European digital sovereignty."[5] The proliferation of LEO with tens of thousands of satellites will require increasing levels of automation to handle intraconstellation operations and to enable future constellation growth and system safety in a given orbital altitude regime.

The creation of megaconstellations is the result of two factors. First, the shift in the commercial space industry to create standardized, rapidly produced, and high-volume space-capable vehicles has caused both the size and cost of individual satellites to decrease drastically.[6] The ability to buy commercial-off-the-shelf components instead of making proprietary hardware lowers the cost of research and development, thus accelerating system production.

The second factor is a function of satellite size. As the satellite form factor decreases, more satellites can fit inside the payload fairing of a single launch vehicle, which, in turn, drives down the cost per satellite to reach orbit. Overall, the costs of satellite design, production, and space launch are decreasing, thus allowing for the nearly exponential proliferation of near-Earth orbital regimes. Consequently, the increase in satellites will lead to an escalation of costs associated with operations if the current satellite control paradigm does not evolve to meet the challenges of proliferated orbits.

The evolution of satellite control from human-in-the-loop commands to automation will require the megaconstellation, in concert with the ground communications networks, to deconflict satellite pass times over receiver antennas at specified ground stations.[7] By definition, a "pass time" is the time each satellite needs to downlink, or transmit, data to the ground antenna, as well as to uplink, or receive, commands from the ground station. Depending on the mission and amount of information transmitted, timing is critical.

In addition, the orbital altitude of a given satellite determines the access durations to each ground antenna: the lower the satellite altitude, the faster the satellite passes over a given point on the ground. This planning will be increasingly important as the communication bandwidths become more crowded due to more satellites flying within the ground receiver's view.

Since the early twenty-first century, an increase in CPU power has enabled the addition of programmable capabilities to onboard satellite subsystems.[8] A growing number of satellites are now being equipped with onboard systems that resemble a standard personal computer.[9] This design architecture, in turn, increases reliability. A satellite's onboard system can now identify and correct for faults and adapt to changing parameters much faster than a human-in-the-loop system.[10] A human-in-the-loop system is comparatively slower due to data transmission and analysis delays and the need for an extra layer of review to verify the correctness and validity of planned operations before command uplink.

One of the most common satellite-control tasks is that of station keeping or maintaining a satellite's predetermined, mission-centric orbital attitude and position. For megaconstellations, an attitude determination and control system may control all station-keeping operations. Due to an increase in ground-station demand resulting from a vastly greater number of contacts, each satellite will have to determine correct orbital attitude and position deviations autonomously to ensure continued constellation stability and mission functionality and to reduce the likelihood of satellite collisions.[11]

Shifting such attitude and orbit maintenance tasks away from the ground segment, however, will require the introduction of a robust fault- and error-alert architecture to identify and notify the human satellite operators of any anomalous events. Ultimately, raising more house-keeping commands into the purview of control automation will shift the satellite maintenance workload from continuous hands-on, day-to-day human operations to an on-call, human-response control structure. Greater automation will also remove the likelihood of an incomplete command sent by human operators or the need to check for unsafe commands before data uplink.[12]

Satellite Control Evolution

While automation will play a large role in handling satellite functions, the main changes for cybersecurity will come from the evolutionary shifts made in the ground-control segments and associated security implementation requirements. In the 2020 Space Capstone Publication *Spacepower: Doctrine for Space Forces*, the foundation for cybersecurity is defined in the cyber operations spacepower discipline as the "knowledge to defend the global networks upon which military space power is vitally dependent," the "ability to employ cybersecurity and cyber defense of critical space networks and systems," and the "skill to employ future offensive capabilities."[13]

The future of security implementation is already being felt on the manufacturing side for DOD contracts. The recently introduced Cybersecurity Maturity Model Certification (CMMC) program pushes the level of responsibility for cybersecurity down, starting with the industries providing the components and systems, then to the Department of Defense by requiring it to use the published National Institute of Standards and Technology rating system.[14] The CMMC is also rooted in the Federal Acquisition Regulation, Federal Information Processing Standards, and general industry collaboration.[15]

The CMMC does have several caveats such as not requiring compliance for commercial-off-the-shelf systems.[16] This shift will ensure the hardware and software introduced for future satellite-control needs will be primed for cyberdefense. Another aspect that will play a role in the coming changes focuses on the protection of potential dual-use technologies. "Entrepreneurs with innovative and potentially dual-use technologies must improve the protection of their intellectual property from unintended foreign assimilation, including protecting their networks from cyber exfiltration attempts, and avoiding exit strategies that transfer intellectual property to foreign control hostile to U.S. interests."[17]

Some of these dual-use technologies can come in the form of software-defined components that will allow for greater flexibilities in upgrading the on-orbit and ground-control segments, especially in the area of communication systems.[18] Though software-defined systems will add increased flexibility and allow for faster fixes if damaged (for example, there is no need to replace expensive parts if the component can be simply reprogrammed), it will also introduce a new level of security requirements and response capabilities due to the inherent vulnerabilities in all software control systems.

Unlike traditional cybersecurity training provided to most Airmen, Guardians may require enhanced cyber skills to manage risk in the space environment. The Space Force chief technology and innovation officer describes USSF as a digital service; accordingly, Guardians will likely need to understand how digital engineering intersects with cybersecurity in order to model complex systems and cyber threats.[19] Guardians will need to be able to conceptualize how existing hardware and evolving software components interact as well as how they may be exploited by threat actors.

Furthermore, they will likely benefit from development, security, and operations training that will help them craft new software components that not only meet mission needs but are continuously hardened in response to evolving threats. Advanced digital twin modeling—a one-for-one virtual model tested in an operationally accurate simulated environment—may provide a feedback loop to inform operators of how well these new software components perform across a risk spectrum.

Another area of evolving satellite control relates to the use of flexible ground control systems, more specifically, the ground antennas used to transmit commands and receive data. Commercial entities such as Microsoft are introducing GSaaS to increase capabilities and offset costs associated with satellite command and control.[20] These systems will need to be diverse in operational software and equipment to cover the wide range of satellite technologies currently used. Alternatively, future satellite designs that intend to use this emerging method of ground control can establish a form of technological standardization. In either case, commercializing the ground segment will help handle the increased volume and bolster networked capabilities.

Despite these benefits, however, current satellite programs base network security on the legacy assumption that ground stations and the associated ground network are program- or owner-controlled, system-specific, and isolated from other networks. A new control structure is only half of the required change—the other half involves changing how and where some of the satellite-control operations and tasks are conducted.

This second change is coming in the form of cloud-based SOCs. As with the software-defined component and commercialized ground stations, cloud-based control will provide a more robust and flexible answer for growing constellations without the need to build costly new mission-specific "brick and mortar" operations centers.[21] This area already has several working examples, such as the "Major Tom" system—produced by the commercial firm Kubos—that is implemented by the Planet company for use in its Dove constellation consisting of approximately 250 small satellites.[22]

Cloud-based systems will have the added benefit of being accessible from any "secure" networked computer. In concert with the aforementioned commercial ground stations, cloud-based systems could enable megaconstellation control from any location on the globe featuring a proper access point.

In the emerging satellite-control dynamic, an example of potential operations starts with a customer satellite sending spacecraft state-of-health or other data to a configured service receiver. The receiver then uploads the data to a cloud-based SOC that is accessible by satellite operators from any networked computer system. Even with this control flexibility, the use of increasingly networked systems owned by third parties, rather than the satellite or constellation operator, can introduce new entry points and areas for cyber vulnerability.[23] To ensure the cyber protection of all US and Allied space-based assets, satellite programs and control architectures directly in touch with these evolving systems will need to change just as drastically as the systems themselves.[24]

Satellite Survivability Considerations

The goal of any satellite system is to maintain mission functionality for the planned mission lifetime; this requires satellite survivability. Satellite survivability is a function of three time-separated phases: susceptibility, vulnerability, and recoverability. Survivability is promoted if a system's susceptibility and vulnerability to natural and/or manmade threats are minimized while the prospect of recoverability is maximized. From a manmade-threat perspective, susceptibility analysis focuses on the threat system and its ability to successfully detect, be employed, intercept, and finally function as intended vis-à-vis the target satellite system.

Similarly, a satellite's vulnerability relates to its ability to survive the threat's intended weapon effects. Finally, recoverability is the ability of a satellite (and the satellite operators), following damage from a threat system, to take emergency action to prevent the loss of the satellite and/or to regain a level of satellite mission capability.[25] These components of survivability can be extrapolated to megaconstellations as a system-of-systems due to their interconnected internal communications and mission architecture.

The Venn diagram (fig. 1) depicts survivability considerations for megaconstellations, outlining the aspects of susceptibility, vulnerability, and recoverability. Overall, the high number of satellites comprising megaconstellations and the use of emerging autonomy and network technologies represent both primary strengths and weaknesses for megaconstellations. While the risk of satellite collision and debris impact constitute a constant environmental risk to operations, megaconstellations are increasingly susceptible to cybersecurity threats due to the use of commercial GSaaS and cloud-based satellite operations.

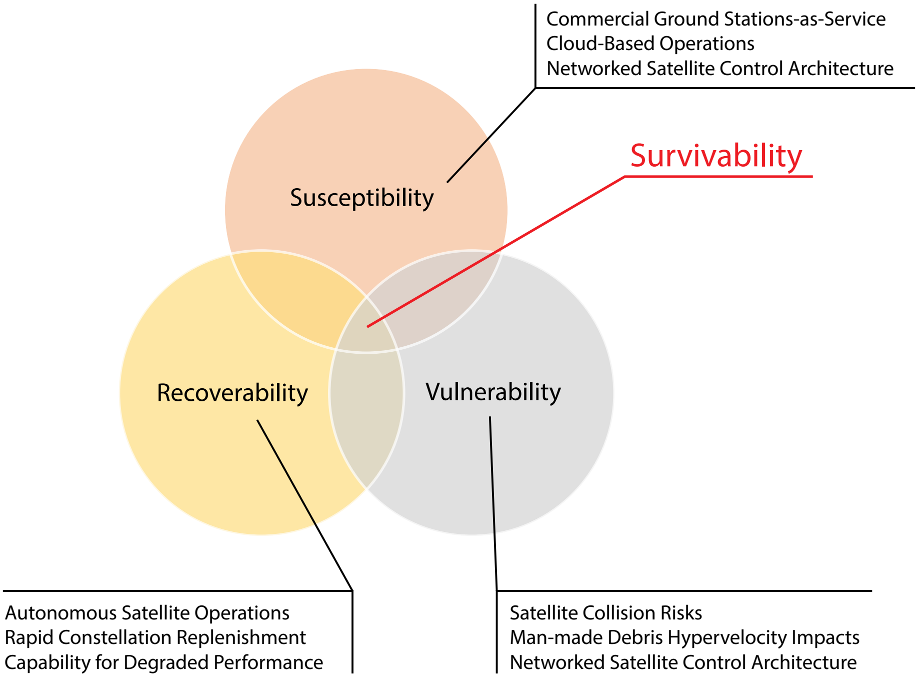

Commercial Ground Stations-as-Service
Cloud-Based Operations
Networked Satellite Control Architecture
Survivability
Susceptibility
Recoverability
Vulnerability
Autonomous Satellite Operations
Rapid Constellation Replenishment
Capability for Degraded Performance
Satellite Collision Risks
Man-made Debris Hypervelocity Impacts
Networked Satellite Control Architecture

Figure 1. Megaconstellation survivability

Cybersecurity threats are varied based on the source of origin and damage mechanism. Satellite operators must maintain a proper understanding of the cyber-threat landscape and the digital and networked functionality of the megaconstellation in order to secure continued mission effectiveness and survivability.

The Networked Operations Center

With anticipated shifts in both methods and infrastructure for space-control operations, there should be an equal shift in the cadre structure and training for satellite-operation teams in the Department of Defense and commercial sectors. On the satellite-operations floor, operators often reach out to fellow team members when anomalous situations arise with satellite systems. But this consultation only works well if the members on both ends of the conversation talk the same language.

As the transition to increasingly networked centers interfacing with highly automated systems progresses, space operations and cybersecurity professionals should learn and understand more of the other members' skill sets and technical terminology. Ideally, the formal training for satellite-operations team members will evolve to include a space- and cyber-centric curriculum. This training could be in the form of introductory classes into cyberdefense for space professionals, and satellite mission design and communications for the cyber professionals.

The USSF is in the crucial position to make this happen starting at the ground level. As mentioned in the Space Capstone Publication, increased education will add to the understanding of the "network dimension."[26] Optimally, this education would result in embedding cyberoperations members at key SOCs, in addition to having increased cybersecurity and monitoring training at all levels of satellite operations. This approach will facilitate a highly digitally capable satellite-operations cadre.[27]

Building a cyber-minded and space-proficient space-control foundation will ensure space and cyberspace professionals will have the tools needed to tackle any future growth in satellite capabilities and space mission execution. It will also empower members with the abilities and confidence to react rapidly and even preemptively to future threats.

Conclusion

Satellite systems and controls architectures are in a rapid state of change. Satellite automation could significantly alter the current hands-on satellite-operations mission to one of key-event monitoring, with a consolidated human-in-the-loop team present to react to and resolve issues that cannot be directly handled by the satellite itself or by the megaconstellation. Additionally, the introduction of a more capable and increasingly flexible mission-operations system, one using emerging technologies such as cloud-based networks and services like privately owned and networked ground stations, will make it possible for true 24/7 global access to and control of satellite systems.

To ensure the continued safety and security of on-orbit satellite systems, both the defense and commercial space sectors must adapt to the rapidly changing digital landscape of future space operations. The introduction of the CMMC has already demonstrated such an adaptation, along with the alignment of emergent USSF doctrine and strategy with cyber-mindedness. The final step will be to shape the future of the USSF and USAF space and cyberspace cadre to be better prepared as a digital force synergistically working to remain at the forefront of protection in the increasingly competitive, contested, and congested domain of space.

As LEO becomes more congested and the mission sets for megaconstellations expand beyond telecommunications, the operating altitudes for megaconstellations will also expand. As a result, the space and cyberspace cadre—Airmen and Guardians alike—must be poised to handle considerations of autonomy and cybersecurity in LEO, geosynchronous Earth orbit, and beyond into the cislunar realm. ✪

Carl Poole

Captain Carl Poole, USSF, is an orbital analyst and holds a master of science from the Air Force Institute of Technology.

Robert Bettinger

Dr. Robert Bettinger, Major, USAF, is an assistant professor of astronautical engineering and curriculum chair for the astronautical engineering degree program at the Air Force Institute of Technology.

Mark Reith

Dr. Mark G. Reith, USAF, retired, is an adjunct professor of systems engineering at the Air Force Institute of Technology.

Notes

[1] J. B. Hartley and P. M. Hughes, "Automation of Satellite Operations: Experiences and Future Directions at NASA GSFC," in *Space Mission Operations and Ground Data Systems - SpaceOps '96, Proceedings of the Fourth International Symposium held 16–20 September 1996 in Munich, Germany*, ed. T. D. Guyenne (Paris: European Space Agency, 1996): 1262–69.

[2] Steven J. Butow et al., *State of the Space Industrial Base 2020: A Time for Action to Sustain US Economic & Military Leadership in Space*, (Washington, DC: USSF, Air Force Research Laboratory, and Defense Innovation Unit, July 2020), http://aerospace.csis.org/.

[3] Jonathan C. McDowell, "The Low Earth Orbit Satellite Population and Impacts of the SpaceX Starlink Constellation," *Astrophysical Journal Letters* 892, no. 2 (2020): 1–18, https://iopscience.iop.org/.

[4] Dan Swinhoe, "China's Moves into Mega Satellite Constellations Could Add to the Space Debris Problem," Data Center Dynamics, April 20, 2021, https://www.datacenterdynamics.com/.

[5] Jonathan O'Callaghan, "Europe Wants to Build Its Own Satellite Mega Constellation to Rival SpaceX's Starlink," *Forbes*, December 23, 2020, https://www.forbes.com/.

[6] Mohamed Khalil Ben-Larbi et al., "Towards the Automated Operations of Large Distributed Satellite Systems, Part I: Review and Paradigm Shifts," *Advances in Space Research* 67, no. 1 (June 1, 2021), https://www.sciencedirect.com/; and Ben-Larbi et al., "Towards the Automated Operations of Large Distributed Satellite Systems, Part II: Classification and Tools," *Advances in Space Research* 67, no. 1 (June 1, 2021), https://www.sciencedirect.com/.

[7] Ben-Larbi et al., "Paradigm Shifts"; Ben-Larbi et al., "Classification and Tools"; Michael J. Bentley, Alan C. Lin, and Douglas D. Hodson, "Overcoming Challenges to Air Force Satellite Ground Control Automation," in *Proceedings of the IEEE Multi-Disciplinary Conference on Cognitive Methods in Situational Awareness and Decision Support (CogSIMA)* (Curran Associates, June 2017), https://ieeexplore.ieee.org/; and Jun Tominaga, José Demísio Simões da Silva, and Mauricio Goncalves Vieira Ferreira, "A Proposal for Implementing Automation in Satellite Control Planning" (paper, SpaceOps 2008 Conference, Heidelberg, Germany, May 12-16, 2008), https://arc.aiaa.org/.

[8] Misa Iovanov et al., "Automation of Daily Tasks Necessary for the Management of a Large Satellite Constellation" (paper, American Institute of Aeronautics and Astronautics (AIAA) Space 2003 Conference & Exposition, Long Beach, CA, September 23-25, 2003), https://arc.aiaa.org/.

[9] Ben-Larbi et al., "Paradigm Shifts"; and Ben-Larbi et al., "Classification and Tools."

10. Gilles Kbidy, "Flying Large Constellations Using Automation and Big Data" (paper, SpaceOps 2016 Conference, Daejeon, South Korea, May 13, 2016), https://arc.aiaa.org/.

11. Jérôme Thomassin, Maxime Ecochard, and Guillaume Azema, "Predictive Autonomous Orbit Control Method for Low Earth Orbit Satellites" (paper, International Symposium on Space Flight Dynamics, Matsuyama, Japan, June 6-9, 2017), https://issfd.org/; and Byoung-Sun Lee, Yoola Hwang, and Hae-Yeon Kim, "Automation of the Flight Dynamics Operations for Low Earth Orbit Satellite Mission Control," in *Proceedings of the 2008 International Conference on Control, Automation, and Systems* (Curran Associates, April 2009), https://ieeexplore.ieee.org/.

12. Ben-Larbi et al., "Paradigm Shifts"; and Ben-Larbi et al., "Classification and Tools."

13. John W. Raymond, *Spacepower: Doctrine for Space Forces*, Space Capstone Publication (Washington DC: USSF, June 2020), 52, https://www.spaceforce.mil/.

14. Barry Rosenberg, " 'Start of a New Day': DoD's New Cybersecurity Regs Take Effect Today,' " Breaking Defense, December 1, 2020, https://breakingdefense.com/.

15. "Understanding the CMMC Fundamentals," Cybersecurity Maturity Model Certfication Center of Excellence, November 26, 2020, https://cmmc-coe.org/.

16. Rosenberg, " 'New Day.' "

17. Butow et al., "Space Industrial Base."

18. M. Manulis et al., "Cyber Security in New Space," *International Journal of Information Security* 20 (2020): 287–311, https://link.springer.com/.

19. Space Force Chief Technology and Innovation Office, *U.S. Space Force Vision for a Digital Service*, (Washington, DC: USSF, May 2021), https://media.defense.gov/.

20. Theresa Hitchens, "Microsoft Boosts Space Services, Partnerships," Breaking Defense, October 20, 2020, https://breakingdefense.com/.

21. Ben-Larbi et al., "Paradigm Shifts"; and Ben-Larbi et al., "Classification and Tools."

22. Kubos, "Major Tom"; and Ben-Larbi et al., "Paradigm Shifts."

23. J. D. Scanlan et al., "New Internet Satellite Constellations to Increase Cyber Risk in Ill-Prepared Industries," (paper, 70th International Astronautical Congress, Washington, DC, October 21-25, 2019).

24. Department of Defense (DOD), *Defense Space Strategy Summary* (Washington, DC: DOD, June 2020), https://media.defense.gov/.

25. Andrew J. Lingenfelter, Joshuah A. Hess, and Robert A. Bettinger, "From Sanctuary to Warfighting Domain: A Space System Survivability Framework," *Aircraft Survivability*, Summer 2021, 7–16.

26. Raymond, *Spacepower, 7.*

27. Charles Pope, "Driven by 'a Tectonic Shift in Warfare' Raymond Describes Space Force's Achievements and Future," SpaceForce News, September 15, 2020, https://www.spaceforce.mil/.

TECHNOLOGY

Directed-Energy Weapons

An Option for Strategic De-Escalation

Alfred Cannin

> *A strategist should think in terms of paralyzing, not killing. . . . And on a still higher plane, psychological pressure on the government of a country may suffice to cancel all the resources at its command—so that the sword drops from a paralyzed hand.*
>
> —B. H. Liddell Hart, *Strategy: The Indirect Approach*

Emerging technological advances have provided multiple nonlethal options to deter, deny, and incapacitate threats posed by new adversaries and changing strategic implications. Directed-energy-weapon (DEW) options demonstrate, via an escalation of force from nonlethal to lethal, a direct targeting capability with a high likelihood of low collateral damage and reduced risk of civilian casualties.

The Joint Intermediate Force Capabilities Office, formerly the Joint Nonlethal Weapons Directorate, is exploring the function and application of nonlethal DEW defense technologies across the spectrum of conventional warfare and the competition continuum. These technologies will allow the US military to accomplish the mission while protecting friendly forces "without unnecessary destruction that initiates or prolongs expensive hostilities."[1] Current binary decision-making solutions limit early nonlethal weapon-escalation possibilities across the entire range of military options.[2]

A Case for Directed-Energy Weapons

As the United States transitions from a well-developed understanding of terrorism and violent extremism to focus on strategic competition, the US military and coalition forces will encounter similar adversary tactics, techniques, and procedures. In both operational environments, proxy belligerents pursue their objectives in irregular warfare battlespaces.[3] Terrorists and violent extremists conduct embedded operations in populated areas to conceal intent, often seeking opportunities to create collateral damage (CD) and civilian casualties (CIVCAS).[4]

As seen in recent operations, US forces have limited conventional weapons' options against hostile actors comingling with noncombatants as these adversaries seek to capitalize on US kinetic operations and CIVCAS reporting.[5] Violent extremist organizations, with the presence of the world's media, take advantage of mistakes and collateral damage by promulgating narratives critical of US kinetic CD and CIVCAS reporting, shaping an "us-or-them" local propaganda message and shifting international opinion.[6]

By portraying the United States as callous and indifferent to the suffering of local populations, this effective guerrilla tactic creates vulnerabilities for the United States and coalition forces. These vulnerabilities are especially problematic when the US military tries to balance offensive operations and self-defense with strategy in conventional operations and across the continuum of strategic competition. Uncertainty about the true nature of civilian casualties in the battlespace means a delay in identifying hostile acts or intent. Under the current rules of engagement (ROE) in Phase III military operations and exacerbated by the inherent compression of time and space, the rapid escalation of force necessitates a preference for lethal conventional kinetic weapons.[7] Often as a result, the comprehensive analysis required to identify and prosecute a threat is limited.

Traditional conventional weapon escalation-of-force scenarios also limit system 1 (fast thinking) and system 2 (slow thinking) cognitive problem analyses used to determine hostile intent.[8] This analytic model is vital in determining hostile intent and calculating associated responses across the full spectrum of military options, from Phase 0 to Phase V and along gray-zone continuums. Moreover, this calculus is made even more complex by the limitations on range capabilities, complex targeting solutions, fog (actual and metaphorical), and the inescapable friction of war.[9]

Directed-energy weapons should be used in conjunction with conventional weaponry to provide friendly forces with various escalations-of-force capabilities, enabling the military to apply the minimum force required for a specific threat versus a one-size-fits-all kinetic solution.[10] This new escalation-of-force operational concept (fig. 1) complements conventional weapons with the sequential and concurrent use of intermediate-force capabilities. Such an operational concept provides the nonlethal and lethal DEW effects that Joint Force commanders require while safeguarding US policy and strategy, limiting adversary retaliation or escalation, and controlling battlespace information and perceptions.

The simplified targeting and speed-of-light characteristics of DEWs provide an increased standoff range for forces, allowing opportunities to prosecute hostile threats early. With a new employment operational concept, DEW capabilities expand the current kinetic escalation-of-force timeline, foster minimum-force weapon applications, and increase safety for friendly forces.

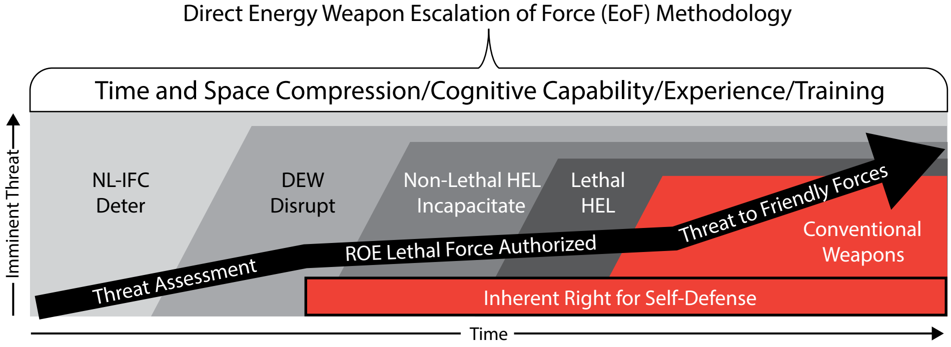

Direct Energy Weapon Escalation of Force (EoF) Methodology
Time and Space Compression/Cognitive Capability/Experience/Training
Imminent Threat
NL-IFC
Deter
DEW
Disrupt
Non-Lethal HEL
Incapacitate
Lethal
HEL
Conventional
Weapons
Threat Assessment
ROE Lethal Force Authorized
Threat to Friendly Forces
Inherent Right for Self-Defense
Time

Figure 1. DEW escalation-of-force methodology

Nonlethal Directed-Energy Weapons

Bridging the gap between military presence and lethal intent, the Joint Intermediate Force Capabilities Office shapes the use of emerging nonlethal microwave, millimeter, and laser-energy technologies in gray-zone operations, urban areas, and irregular and unconventional warfare battlefields.[11] Nonlethal DEWs are "developed and used with the intent to minimize the probability of producing fatalities, significant or permanent injuries, or undesired damage to material or infrastructure."[12] Nonlethal DEW technologies safeguard US forces against nefarious activities with capabilities including long-range, laser-induced plasma audio devices that communicate US military presence, and nonlethal dispersal and denial devices, which are silent and invisible to the human eye.[13]

Additionally, silent, often nonattributable, nonlethal millimeter and microwave devices exist to disorient personnel and disable, neutralize, and incapacitate enemy electronic targets such as threat vehicles, vessels, and aircraft, with mitigation benefits similar to those noted above for the escalation-of-force concept.[14] Nonlethal

DEW options could better address a potential hostile act in uncertain battlespaces—urban—precluding an automatic, and possibly unnecessary, acceleration to lethal-targeting options.

Lethal Directed-Energy Weapons

Lethal DEW, including high-energy lasers (HEL), complement nonlethal DEW diffuse capabilities in the escalation-of-force methodology, progressing from nonlethal intermediate-force capabilities to material-kill targeting. These DEWs are "technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles."[15] These technologies are developed into weapons or systems "that use directed energy to incapacitate, damage, or destroy enemy equipment, facilities, and/or personnel."[16]

Silent and invisible, high-energy laser systems used on countermaterial targets can disable and destroy the mobility of positively identified personnel, minimizing conventional-weapon escalation and the secondary threat of collateral damage and civilian casualties.[17] High-energy lasers are in the nascent stage of development and not currently authorized. But as their power levels evolve, weapon-quality lethal targeting options will emerge.[18]

Advantages

Directed-energy weapon technologies offer a simplified aiming solution and instantaneous targeting escalation from nonlethal intent to lethal force, resulting in an elongated nonlethal weapons escalation-of-force window. If applied early, nonlethal and lethal DEWs "in certain cases prevent the use of excessive force, escalation in hostilities, and CD."[19] Lethal DEW effects, highly discriminant and anti-suffering, offer a solution to minimize critical infrastructure or private property collateral damage while still accomplishing military and political objectives. These weapons also remove the violent sensation and perception associated with conventional kinetic weapons, avoiding third-order effects of adversary information-operations propaganda and messaging that facilitates support and recruiting.[20]

Over time, as the size, weight, power, and cooling levels of DEWs advance, flexible nonlethal and lethal DEWs are anticipated to proliferate across a diverse range of security environments. These capabilities could be employed more routinely than any other conventional weapon or emerging-weapons technologies.[21]

The Right Tool

With various overlapping 5-Ds (deny, degrade, disrupt, deceive, or destroy) properties, the preemptive escalation-of-force application of DEWs could resolve malicious activities before conventional lethal force is required. The early application of nonlethal weapons de-escalates ambiguous situations with minimum use of force, safeguarding friendly forces while avoiding CD and CIVCAS. These weapons can be applied sequentially and concurrently during the escalation of force to demonstrate resolve while avoiding damage caused by conventional kinetic (blast, fragmentation, cratering, incendiary, and penetration) weapons.

During confrontations where the ROE authorize lethal force, violence is not always immediately suitable across the range of military options, particularly in gray-zone operations where US policy and strategy limit military operations below the threshold of armed conflict. The civilian population-centered approach facilitated by nonlethal DEWs retains the hearts and minds of those the United States defends and helps gain the long-term trust and confidence of future populations facing irregular and unconventional warfare in these unstable gray-zone battlespaces of great power competition.[22]

The scalability, silent, and often nonattributable nature, damage-level selections, and immediate responsiveness (speed of light) of DEW capabilities provide friendly forces the means to target nuisance cominglers and direct threats with a variety of tailored, minimum-force weapons.[23] Nonlethal and lethal DEW capabilities also allow for engineered warfare scenarios. The combination of effects could greatly influence multiple wartime missions and result in less cause for the enemy to retaliate or escalate force. With no clear evidence of US force and attribution or signature-less employment by friendly forces, the United States can engineer the de-escalation of a potential enemy threat.

Great power competition proxies deliberately operate below the threshold of armed conflict, rendering conventional kinetic weapons incompatible as they can "adversely affect efforts to gain or maintain legitimacy and impede the attainment of both short-term and long-term goals."[24] The use of intermediate-force capabilities, nonlethal DEWs, and the nonlethal application of HELs are particularly advantageous in gray-zone scenarios "when restraints on friendly weaponry, tactics, and levels of violence characterize the operational environment" across the competition continuum.[25]

Although the 2017 *National Security Strategy*, 2018 *National Defense Strategy*, and 2021 *Interim National Security Strategy* have refocused the Department of Defense toward strategic competition, the nature of warfare and our adversaries' tactics, techniques, and procedures (to operate as a wolf in sheep's clothing, maneuvering to induce CD and CIVCAS events that can then be exploited to the disadvantage of the United States) remain unchanged.[26]

Military forces operate across the spectrum of conflict zones, including military operations other than war. During such noncombat operations, the authorized use of nonlethal DEWs early in an escalation-of-force methodology increases the envelope of time available to identify and mitigate a threat. This capability provides Joint Force commanders the technological advantage to ensure friendly-force safety with mission success across multiple spectrums.

Alternative Consideration

Implementing DEWs, individually and as a whole, will involve the expected hurdle of doctrine, organization, training, materiel, leadership, personnel, facilities, and policy, and necessary bureaucracy. But DEWs will also face external scrutiny. Some argue the premature, ultimately disappointing DEW technologies in the Department of Defense are based not on results but instead on overestimated technological capabilities and unrealistic timelines.[27] Others amplify this warning, noting future budgetary constraints, challenges in adopting innovation, and disconnects in implementation as the United States fails to capitalize on Ally and partner relationships, particularly in DEW technologies.[28]

The effects of public opinion on US decision makers are an unanticipated obstacle to the implementation of existing DEWs. Highlighted by the US and international media, multiple human-rights activists and critics have raised two fundamental issues regarding DEW effects—safety concerns and ethics violations.[29]

Culminating in 2010, controversy obscured the capabilities of the Active Denial System in Afghanistan.[30] Major media headlines hypersensationalized the effects of active-denial-system weapons—in this case a microwave heat ray gun dubbed *Silent Guardian*—as crippling and brutally painful, like "being exposed to a blast furnace," or "making people feel like they are on fire."[31] These only partially substantiated media spins resulted in the immediate removal of the Army active-denial system weeks after its arrival but before its operational use—drastically stunting the progress and momentum of DEW implementation.[32]

The effectiveness of the media campaign directly conflicts with the hypothesis that nonlethal DEWs promote strategic benefits and tactical prudence.[33] The effects of public opinion also highlight future requirements to purposely incorporate supportive narratives that encourage the adoption and implementation of DEW, which include re-educating decision makers on past misunderstandings and current capabilities.

Conclusion

New and old adversaries alike seek to exploit political perceptions regarding the use of force. Changing US priorities have led to new challenges that modern technologies and innovative tactics could address, providing Joint Force commanders the tools to achieve military objectives and ROE authorities to execute minimum-force effects. Directed-energy weapons, including intermediate-force, nonlethal, and lethal capabilities, present a complementary set of useful minimum-force options as the US military continues to operate across multiple spectrums of conflict, especially in urban environments.

Updated escalation-of-force guidance in the form of ROEs that leverage DEW capabilities early could enable Joint Force commanders to proactively shape battlefield conditions and avoid unnecessarily raising the level of conflict. These weapons could mitigate second- and third-order effects of irreversible US kinetic weapon miscalculations, thus safeguarding US strategy and political objectives, limiting adversary retaliation, and shaping battlespace information, influence, and perceptions in conventional operations and across the continuum of strategic competition.[34]

Additional research should aim to quantify if effects across multiple spectrums of conflict can offset conventional weapon incompatibilities, de-escalate battlefield scenarios, deter adversaries, and shape battlespace information, influence, and perceptions. Furthermore, research must address the current escalation-of-force model, coercion, first-use policies, and just war theory to validate benefits for an early escalation-of-force methodology. Moreover, a clearly articulated DEW science and technological understanding, a cost-benefit analysis, and the merging of Joint Intermediate Force Capabilities Office intermediate-force capability doctrine with HELs will encourage policy makers and DOD leadership to adopt and implement these emerging DEW capabilities. ✪

Alfred Cannin

Major Alfred Cannin, USAF, a winged aviator in USAF Special Operations Command, holds a master of aerospace science from Embry-Riddle Aeronautical University.

Notes

[1] Wendell B. Leimbach, interview with author, September 16, 2020.

[2] Sjef Orbons, "Are Non-Lethal Weapons a Viable Military Option to Strengthen the Hearts and Minds Approach in Afghanistan?" *Defense & Security Analysis* 28, no. 2 (2012): 114–30.

[3] Department of Defense (DOD), *Summary of the Irregular Warfare Annex to the National Defense Strategy* (Washington, DC: DOD, 2020).

[4] Stephen D. Davis, "Controlled Warfare: How Directed-Energy Weapons Will Enable the US Military to Fight Effectively in an Urban Environment While Minimizing Collateral Damage," *Small Wars & Insurgencies* 26, no. 1 (January 2015): 49–71.

[5] Davis, "Controlled Warfare," 49–71.

[6] Orbons, "Non-Lethal Weapons," 127.

[7] Orbons, "Non-Lethal Weapons."

8. Paul K. Van Riper, "The Identification and Education of U.S. Army Strategic Thinkers," in *Exploring Strategic Thinking: Insights to Assess, Develop, and Retain Army Strategic Thinkers*, ed. Heather M. K. Wolters, Anna P. Grome, and Ryan M. Hinds (Fort Belvoir, VA: US Army Research Institute for the Behavioral and Social Sciences, February 2013), 16–18, https://doi.org/10.1037/e639722013-001; and Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).

9. Chairman of the Joint Chiefs of Staff (CJCS), *Joint Planning*, Joint Publication (JP) 5-0 (Washington, DC: CJCS, December 1, 2020), https://www.jcs.mil/; and Caleb Carr, ed., *The Book of War* (New York: Modern Library, 2000).

10. CJCS, *Peace Operations*, JP 3-07.3, Incorporating Change 1 (Washington, DC: CJCS, October 22, 2018), GL-4, https://www.jcs.mil/.

11. Orbons, "Non-Lethal Weapons."

12. Ashton B. Carter, *DoD Executive Agency for Non-Lethal Weapons (NLW), and NLW Policy*, DOD Directive 3000.03E, Incorporating Change 1 (Washington, DC: DOD, September 27, 2017), https://fas.org/.

13. Davis, "Controlled Warfare"; and Leimbach, interview with author.

14. Davis, "Controlled Warfare"; and Leimbach, interview with author.

15. DOD, *DoD Dictionary*, s.v. "directed energy," accessed July 31, 2021, https://www.jcs.mil/.

16. DOD, *DoD Dictionary*, s.v. "directed energy weapon," accessed July 31, 2021, https://www.jcs.mil/

17. Davis, "Controlled Warfare."

18. "Solid-State High-Energy Laser Systems," Northrop Grumman (blog), November 9, 2020, https://www.northropgrumman.com/.

19. Davis, "Controlled Warfare," 63.

20. Davis, "Controlled Warfare," 49.

21. James N. Mattis, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Office of the Secretary of Defense, January 2018), https://dod.defense.gov/; and Northrop Grumman, "Laser Systems."

22. Orbons, "Non-Lethal Weapons."

23. Joint Targeting School (JTS), *Joint Targeting School Student Guide* (Dam Neck, Virginia: JTS, March 1, 2017), https://www.jcs.mil/; Orbons, "Non-lethal Weapons"; Davis, "Controlled Warfare"; and Leimbach, interview with author.

24. Rudolph C. Barnes, "Military Legitimacy in OOTW: Civilians as Mission Priorities," *Special Warfare* 12, no. 4 (Fall 1999): 38–39.

25. CJCS, *Joint Targeting*, JP 3–60 (Washington, DC: CJCS, 2013), II–16.

26. Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: Executive Office of the President, December 2017), https://trumpwhitehouse.archives.gov/; and Mattis, *National Defense Strategy.*

27. Ash Rossiter, "High-Energy Laser Weapons: Overpromising Readiness," *Parameters* 48, no. 4 (Winter 2018–19): 33–44, https://press.armywarcollege.edu/; and John Gourville, "Eager Sellers and Stony Buyers Understanding the Psychology of New-Product Adoption," *Harvard Business Review* (June 2006), https://hbr.org/.

28. Rossiter, "High-Energy Laser"; and Hugh Beard, "View from the UK: Directed Energy as a Next Generation Capability," (address, Booz Allen Hamilton 2019 Directed Energy Summit, n.d.), https://www.boozallen.com/.

29. Sharon Weinberger, "US Military Heat-Ray: Set Phasers To . . . None," BBC News, November 18, 2014, https://www.bbc.com/.

30. Weinberger, "Military Heat-Ray."

31. Tim Elfrink, "Safety and Ethics Worries Sidelined a 'Heat Ray' for Years. The Feds Asked about Using It on Protesters," *Washington Post*, September 17, 2020, https://www.washingtonpost.com/; and John Hudson, "Raytheon Microwave Gun Recalled Amidst Controversy," *Atlantic*, July 19, 2010, https://www.theatlantic.com/.

32. Elfrink, "Safety and Ethics"; and Noah Shachtman, "Pain Ray Recalled," *Wired*, July 20, 2018, https://www.wired.com/.

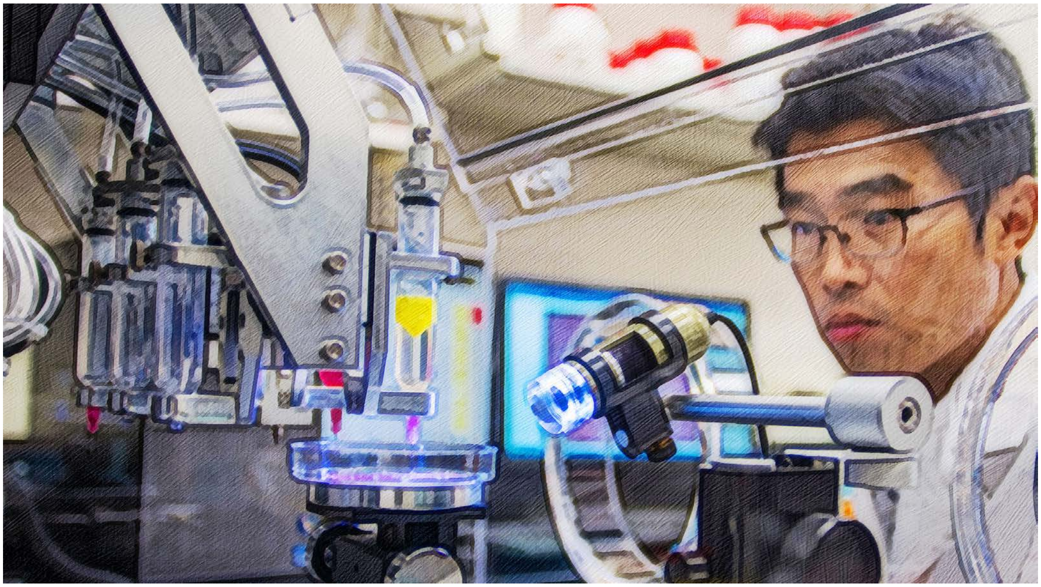
33. Schachtman, "Pain Ray Recalled"; and Orbons, "Non-Lethal Weapons."

34. JTS, *Student Guide*.

TECHNOLOGY

Mobilizing Uniformed Scientists and Engineers

Brian J. Fry



Connecting what combat forces need with what technology can provide has been an enduring problem, one that will become increasingly urgent to resolve.[1] Crossing this divide will require leaders with a deep understanding of science and engineering and the ingenuity to apply this understanding to operational problems. Here the Air Force has an opportunity to reassess the role of a talented mix of officers capable of making that technical-operational link, but whose utility often seems uncertain or hazy—uniformed scientists and engineers (S&Es). (Hereafter, "S&Es" refers only to uniformed military officer scientists and engineers.)

Background

The Air Force chief of staff has declared that accelerating change is the service's strategic imperative.[2] In part, this imperative applies to advancing technology the Air Force relies on heavily for dominance and is reminiscent of the technological challenges the US military faced at the dawn of World War II.[3] In that war, the US military and the US Office of Scientific Research and Development fielded a dazzling array of new technologies by mobilizing civilian scientists and engineers from academia and industry. But doing the same for S&Es was much more problematic.[4] A 1948 Department of the Army study examined the utilization of S&Es during World War II and found that despite a wealth of uniformed scientific and engineering expertise, a significant portion—more than 36 percent—had been squandered in jobs poorly utilizing that expertise or in jobs that used none of it. In fact, less than 30 percent of S&Es were placed in billets in which their expertise was described as "well utilized."[5]

The study recognized the importance of S&Es within the military services, noting that "any future war will require within the Services a large group of technically trained officers of high skill to function in research, planning, and operations."[6] Yet in the decades since, numerous other studies have found the same issues and concerns voiced by S&Es in the 1940s remain true today: S&Es are not doing actual science and engineering, there is poor technical leadership, and advanced degrees are ignored or poorly utilized.[7]

Throughout the history of the service, a common sentiment has maintained that the Air Force has untapped science and engineering expertise within its uniformed ranks. The difference today is that the US military no longer enjoys the enormous technological lead it once did, despite investing billions of dollars in research and development.[8] As detailed in the 2018 *National Defense Strategy*, increasingly rapid and diverse advancements in technology require the military to utilize its people (particularly S&Es) better in order to more effectively employ technology.[9]

Mobilizing Air Force S&Es

While there are examples of the Air Force successfully tapping into its uniformed technical talent during World War II (our last peer-level conflict) and the Cold War (our last peer-level competition), perhaps the strongest contemporary example of lucrative employment of S&Es is the Israeli Defense Forces' (IDF) Talpiot program.[10] This program trains participants in a rigorous science, technology, engineering, and mathematics curriculum in addition to a broad spectrum of training with operational forces.[11] Before graduation, participants complete a thesis project proposing a technical solution to a military need they identified during training.[12]

Despite a budget that is a fraction of the US military's, the IDF, through the Talpiot program, fields technology that is impressive in terms of quality, timeliness, and combat effectiveness (for example, the Iron Dome and Trophy defense systems).[13] The Talpiot program's successes were possible in part because of the program's ability to provide operational experiences complemented by a rich, technical understanding—with the expectation that technical expertise will be applied therein—directed toward creating a cadre of military innovation leaders.

Against a peer adversary, the United States must field and employ new technologies faster and more effectively than the opponent. One expert recently noted the divide "between academic scientists, national research labs, industrial research labs, and the military" and the historic impacts of the military failing to identify and field game-changing technologies.[14] To address this deficiency, he advocated for servicemembers with the unique "ability to translate and mediate between the creators of new technologies and the users of those technologies."[15] Within the Air Force, S&Es with operational expertise are already poised to fill this role.

Air Force scientists—biologists, chemists, physicists—and engineers—aeronautical, computer, electrical, mechanical, flight test—are responsible for analyzing, researching, developing, and testing new technologies and are also tasked with supporting highly technical operations and intelligence.[16] Entry into these career fields requires a science or engineering baccalaureate degree. These academic credentials combined with their career field responsibilities, operational experience tours, and their status as uniformed officers, provide S&Es the foundational elements to build the rapid technology transition capability enjoyed by the IDF and advocated for by experts in the field.[17]

Although the building blocks are there, the Air Force's current employment of S&Es is ripe for improvement. Some S&Es are assigned to billets that utilize their technical expertise but only at the junior ranks, typically before they obtain graduate degrees that would enable greater participation in and contributions to technical activities.[18]

Ideally, an S&E would earn an advanced technical degree early in their career. But this pursuit often receives lukewarm encouragement, and few senior command opportunities are designated for S&Es with these credentials.[19] From a career field management perspective, many S&Es are viewed as interchangeable with acquisition managers. They often serve in system program offices as part of an integrated product team responsible for tracking the cost, schedule, and performance aspects of a research and development contract.[20]

Placing S&Es in these positions has value, but due to the delay in obtaining graduate degrees, lack of promotion incentives for advanced technical degrees, and mismatches between specialty and assignment, frequently S&Es lack sufficient technical depth/specialization to hold defense contractors technically accountable.[21] Consequentially, S&Es are utilized in nontechnical activities, further obfuscating the role (and likely hindering the development) of S&Es.[22] Furthermore, from a service-level view, even the existence of S&Es in the Air Force often seems unnecessary: why employ S&Es when government civilian and contractor scientists and engineers have more technical depth and specialization?

This combination of issues aggravates the decades-old challenge of fielding new technologies at the speed of relevance, which is crucial to maintaining a technological edge against peer adversaries. Untangling how S&Es can best be employed to maximize their potential and that of the Air Force requires answering two fundamental questions: (1) How can S&Es be utilized to maximize their and the larger acquisition community's contributions to delivering technology and improving the combat effectiveness of the US military? and (2) What attributes and development do S&Es need to maximize their potential?

Answering these questions will lead to a coherent vision for the S&Es' role and framework for their development, provide unique contributions to the acquisition community, and increase the combat effectiveness of the Air Force. The proposed solutions are not an attempt to cure all that ails Air Force acquisitions. Rather, the article explains the most effective way to employ one component—S&Es—of that apparatus. If the call to action is to "accelerate change," then the Air Force should ensure S&Es are in a position to do so.[23]

The Role of S&Es

In determining how best to utilize S&Es, it is important to consider the attributes of the various professions delivering technology to the Air Force—S&Es, uniformed acquisition managers, and government civilian and contractor scientists and engineers—so the result will excite each of their strengths yet minimize overlap.

Uniformed scientists and engineers are part of the acquisition career group that includes six utilization fields [their two-digit specialty code]: (1) scientific [61], (2) developmental engineering [62], (3) acquisition management [63], (4) contracting [64], (5) finance [65], and (6) senior materiel leader-upper echelon [60] (only for certain colonel positions).[24] This discussion focuses on the first three fields.

Within their respective disciplines, scientists "build understanding" (~350 total officers), engineers "build and test things" (~3,200 total officers), and acquisition managers "buy things" (~2,500 total officers).[25] As a consequence, S&Es are more technically-oriented than acquisition managers: while S&Es must earn a science or engineering degree for entry into their career fields, acquisition managers may possess any undergraduate degree—approximately 20 percent of new entrants possess a science or engineering degree.[26] Additional technical education is also considerably different across the career fields: for instance, roughly 25 percent of scientists and 10 percent of engineers have doctorates (mostly in technical fields), while about 1 percent of acquisition managers possess doctorates.[27]

Government civilian and contractor counterparts to S&Es generally have more specialization in and longevity on technical subjects—sometimes decades—than S&Es who often have just two- to four-year assignments. But while government civilians and contractors can deploy (for example, the Air Force Engineering and Technical Services program), it is not a guaranteed capability or requirement.[28] Moreover, civilians necessitate special considerations, and deploying contractors normally incur significant costs.[29]

Also, while government civilian and contractor scientists and engineers often have or can gain operational expertise, the process is usually via proximity or repeated exposure over a long time period rather than by first-hand experience. Moreover, civilian education institutions seldom include military applications of scientific principles in their curricula.

A distinguishing characteristic of uniformed military service is the implicit expectation to command and to deploy to combat theaters. These S&Es, as well as uniformed acquisition managers, can fill operational career-broadening positions—intelligence, cyber, or maintenance officer tours—that give them first-hand operational experiences they can apply in conjunction with their technical expertise.

Although several professions in the military are charged with providing new technologies, S&Es are the only professions that combine technical expertise, an operational perspective, and the implied expectation to deploy and command. As a result, S&Es can link technical possibilities to operational realities and exploit that connection faster than an adversary. The primacy of linking technical possibilities to operational and command realities (particularly in a combat theater) is what makes the roles of S&Es unique in comparison to uniformed acquisition managers, government civilians, and contractors.

This distinction profits from the S&E's technical expertise compared to the education expected of typical acquisition managers but does not duplicate the specialization of government civilians and contractors. Instead, S&Es use their technical expertise to integrate the expertise of government civilians and contractors, incorporate that knowledge into operational situations, and capitalize on opportunities with timely and impactful technology.

The optimal settings for utilizing S&Es would enable them to apply their technical skills to take advantage of technology through tasks such as conducting research, development, testing, and evaluation of new technology; designing, prototyping, and manufacturing equipment with new technology; facilitating technology transition to field units; adapting existing technology to new uses; analyzing, reverse-engineering, and countering adversary technology; or simply "MacGyver"-ing together something with duct tape and a Swiss Army knife in theater when the adversary has compromised first-line systems.

Exploiting technology *could* include managing a contract developing a new device (status quo for most S&Es today), but that should not be the only method, nor should it be assumed to be the primary method. This entire menu of tasks should be available to S&Es and focused at creating operational advantages. While S&Es could perform these tasks in a variety of locations, making the most of technology in a combat theater is critical.

Countering Peer Adversaries

In order to guarantee decisive advantages on the battlefield, the Air Force must create, field, and employ technologies more effectively than an adapting adversary. The transformative impacts from the introduction of aircraft to warfare in the early twentieth century are a testament to the importance of creating new technologies. Likewise, today's innovative technologies must be contracted, produced, and placed into service—consider the United States' delay in fielding radar systems and Germany's inability to field enough jet aircraft during World War II.[30]

Employing that technology effectively, however, is equally important. Doctrinal frameworks like that produced by the Air Corps Tactical School and eventually the Cold-War-era AirLand Battle allowed aircraft to be viewed not simply as a novelty but as an integrated component necessary to the success of an operational campaign.[31]

To address these operational imperatives, S&Es' war-fighting obligations are:

- **Creating:** S&Es are the source of new war-fighting domains. Air, space, electronic, and cyber warfare began as science and engineering pursuits. These officers seek out technologies that expand on what is possible within existing domains and pursue transformative technologies that extend beyond the limitations of these domains.

- **Fielding**: S&Es are fighting current and future conflicts simultaneously. Essentially S&Es are waging a long-term logistics battle to field new technologies.

- **Employing:** S&Es fight using information. Just as operations researchers use data and analysis and weather officers use their knowledge of the weather, S&Es use their knowledge to discover new information previously hidden and create tools that take advantage of their knowledge. S&Es understand how new technology works and how it can influence the operational environment.

In great power competition, it is insufficient to focus solely on creating and purchasing new technology (where the capabilities of uniformed acquisition managers and government civilian/contractor scientists and engineers may be more advantageous than S&Es). In conjunction with these efforts, the US military must quickly identify those technologies and means of employment that will produce the greatest advantage; the S&Es' blend of technical and operational expertise can accelerate this identification.

If S&Es are to fulfill their war-fighting obligations and their role of exploiting technology faster than an adversary by connecting the technical to the operational, then skilled S&Es should be:

- **Technically proficient**. These officers should have a deep knowledge of their discipline and specialty. Technical proficiency includes an in-depth theoretical understanding—primarily through academic degrees—and practical understanding developed through hands-on experience applying technical skills to practical problems via research and testing. Theory provides the tools S&Es need; practice gives them the opportunities to use those tools. Both elements are needed to provide a well-rounded understanding of their disciplines.

- **Operationally relevant**. These officers should be able to understand and apply technical knowledge in operational and command contexts. Knowledge of the operational environment is necessary for S&Es to fully grasp the constraints such an environment will impose upon their technology. This insight could be gained through discussions with operational units, but working directly with operational units or having first-hand experiences in operations would give S&Es a much more comprehensive understanding of those constraints.

- **Leaders**. These officers should have skills in the following areas: (1) directing a research or test effort; (2) developing doctrine for new technology with operators; (3) advising senior leaders on the relative importance of detailed analyses and requirements; and (4) sharing their knowledge to cultivate junior S&Es, enrich their peers' expertise, and collectively enhance the technical aptitude of the total force. Uniformed scientists and engineers must be able to direct other scientists and engineers toward a technical mission and develop and mentor junior officers to one day succeed them. In this way, S&Es will enable accelerating the technological and doctrinal change necessary for the Air Force to maintain its dominance.

Conclusion

During a conflict with a peer adversary, S&Es can create, adapt, and employ technology to seize opportunities and counter the adversary's efforts, particularly in theater. Developing leaders with deep technical understanding and with experiences applying that technical knowledge to operations has been extremely beneficial for the IDF. The Air Force could similarly benefit from developing its S&Es along the same philosophy.

The union of technical and operational expertise within an officer is a role for which S&Es are educated and professionally developed. Empowering S&Es to be technically capable and operationally relevant will ensure they identify and exploit technical opportunities over our competitors much earlier, infuse an operational mindset in acquisition organizations from the ground up, lead those acquisition organizations with a war-fighting perspective, and perpetuate and accelerate the change necessary to keep the Air Force at the forefront of technology. ✪

Brian J. Fry

Lieutenant Colonel Brian J. Fry, USAF, is a physicist and a US Air Force Academy assistant professor. Dr. Fry is also a member of the Air Force Science and Technology 2030 Strategy Implementation Team.

Notes

1. Winston S. Churchill, *The World Crisis, 1911–1918*, vol. 2 (London: Odhams, 1938), 1442.

2. Charles Q. Brown Jr., *Accelerate Change or Lose* (Washington, DC: Headquarters, US Air Force (USAF), August 2020), 3, https://www.af.mil/.

3. G. Pascal Zachary, *Endless Frontier: Vannevar Bush, Engineer of the American Century* (New York: Free Press, 2018), chap. 3, Kindle.

4. Zachary, *Endless Frontier*, chaps. 7-12; and Headquarters, Department of the Army (HQDA), *Scientists in Uniform, World War II* (Washington, DC: HQDA, 1948), vii–ix, https://babel.hathitrust.org/.

5. HQDA, *Scientists in Uniform*, 11.

6. HQDA, *Scientists in Uniform*, 64.

7. HQDA, *Scientists in Uniform*, 16–17, 61–62; Derek W. Beck, "An Analysis of Retention Issues of Scientists, Engineers, and Program Managers in the U.S. Air Force," (master's thesis, Massachusetts Institute of Technology, February 2005), 198–200, https://dspace.mit.edu/; National Research Council of the National Academies (NRC), Division on Engineering and Physical Sciences and Air Force Studies Board, Committee on Owning the Technical Baseline in the U.S. Air Force, *Owning the Technical Baseline for Acquisition Programs in the U.S. Air Force: A Workshop Report* (Washington, DC: The National Academies Press, 2015), 16, https://doi.org/; and Montgomery C. Hughson, "The Future Role of the USAF Technical Officer," (research paper, Air Command and Staff College, Air University, April 2000), 5–6, 28, 32, https://apps.dtic.mil/.

8. House Armed Services Committee, *Future of Defense Task Force Report 2020*, 116th Cong., 2nd sess., September 23, 2020, 5, https://armedservices.house.gov/.

9. James N. Mattis, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Office of the Secretary of Defense, January 2018), https://dod.defense.gov/, 1; John Shanahan and Laura Junor, "We Need a Goldwater-Nichols Act for Emerging Technology," *Defense One*, December 16, 2020, https://www.defenseone.com/; and USAF, *Science and Technology Strategy: Strengthening USAF*

Science and Technology for 2030 and Beyond (Wright-Patterson AFB, OH: USAF, April 2019), https://www.af.mil/.

10. Benjamin W. Bishop, "Jimmy Doolittle: Cincinnatus of the Air," (dissertation, School of Advanced Air and Space Studies, Air University, July 2016), 102–13, https://apps.dtic.mil/; and "General Lew Allen Jr.," USAF (website), September 1981, https://www.af.mil/.

11. George M. Dougherty, "Accelerating Military Innovation: Lessons from China and Israel," *Joint Force Quarterly* 98, no. 3 (3rd Quarter 2020): 10–19, https://ndupress.ndu.edu/.

12. Dougherty, "Accelerating Military Innovation," 14–15.

13. Dougherty, "Accelerating Military Innovation," 11.

14. Safi Bahcall, "The Case for a Unified Future Warfare Command," War on the Rocks, February 19, 2020, https://warontherocks.com/.

15. Bahcall, "Unified Future Warfare."

16. Headquarters Air Force Personnel Center (HQ/AFPC), *Air Force Officer Classification Directory (AFOCD)* (San Antonio, TX: HQ/AFPC, April 30, 2020), 209–12, http://www.milvet.state.pa.us/.

17. HQ/AFPC, *AFOCD*, 209–17, 267–69.

18. Robert H. Cohn, "Scientist and Engineer Career Patterns for Air Force Civilians and Officers," (Maxwell AFB, AL: Air Command and Staff College, April 1999), 7–10, https://apps.dtic.mil/.

19. Beck, "Retention Issues," 200.

20. Anita Eigner Latin, "Developing Air Force Acquisition Leaders for the 21st Century," (research project, US Army War College, March 12, 2003), 4, https://apps.dtic.mil/.

21. Beck, "Retention Issues," 196, 198; and NRC, *Owning the Technical Baseline*, 1, 12, 16.

22. NRC, *Examination of the U.S. Air Force's Science, Technology, Engineering, and Mathematics (STEM) Workforce Needs in the Future and Its Strategy to Meet Those Needs* (Washington, DC: National Academies Press, 2010), 83, https://doi.org/.

23. Brown, *Accelerate Change or Lose*, 3.

24. HQ/AFPC, *AFOCD*, 207–26.

25. "Air Force Interactive Demographic Analysis System (IDEAS)," Retrieval Applications Web (RAW), AFPC (website), October 2020 dataset, https://www.afpc.af.mil/.

26. HQ/AFPC, *AFOCD*, 267–69.

27. IDEAS.

28. Molly Dunigan et al., *Expeditionary Civilians: Creating a Viable Practice of Department of Defense Civilian Deployment*, RR-975-OSD (Santa Monica, CA: RAND Corporation, 2016), 1–8, https://www.rand.org/.

29. "Air Force Engineering and Technical Services Factsheet," Eielson AFB, AK (website), November 2006, https://www.eielson.af.mil/; Elle Ekman, "Here's One Reason the U.S. Military Can't Fix Its Own Equipment," *New York Times*, November 20, 2019, https://www.nytimes.com/; Federal Trade Commission (FTC), "Comment Submitted by Major Lucas Kunce and Captain Elle Ekman," FTC-2019-0013-0074, FTC (website), September 15, 2019, https://beta.regulations.gov/; and Scott Amey, "DoD Contractors Cost Nearly 3 Times More than DoD Civilians," Project on Government Oversight (website), November 30, 2012, https://www.pogo.org/.

30. Safi Bahcall, *Loonshots: How to Nurture the Crazy Ideas that Win Wars, Cure Diseases, and Transform Industries* (New York: St. Martin's, 2019), 18–19; and Walter J. Boyne, "Goering's Big Bungle," *Air Force Magazine*, November 1, 2008, https://www.airforcemag.com/.

[31] Howard D. Belote, "Warden and the Air Corps Tactical School: What Goes around Comes around," *Airpower Journal* 8, no. 3 (Fall 1999): 39–47, https://www.airuniversity.af.edu/; and John L. Romjue, "The Evolution of the Airland Battle Concept," *Air University Review* 35, no. 4 (May-June 1984): 4–15, https://www.airuniversity.af.edu/.

F-35 O-Ring Production Functions versus Mosaic Warfare

Some Simple Mathematics

Jörg Schimmelpfennig

Introduction*

On January 28, 1986, the space shuttle *Challenger* broke apart 73 seconds into its flight, claiming the lives of all seven astronauts aboard. The Presidential Commission on the Space Shuttle Challenger Accident, known as the *Rogers Report*, identified the failure of rubber O-rings sealing the joints in one of the boosters as the cause of the accident: "The specific failure was the destruction of the seals that are intended to prevent hot gases from leaking through the joint during the propellant burn of the rocket motor."[1] The external tank was destroyed, leading to the breakup of the orbiter.

Tragically, the possibility of an O-ring failure had been known for some time but was not properly communicated. Although the original cause of the disaster was a faulty design, the immediate cause—defective O-rings costing just a couple of dollars—lent its name to Michael Kremer's idea of an O-ring production function.[2] In contrast to the classical view of output as a deterministic function of some inputs, production is viewed as consisting of a wide range of independent subsystems all prone to failure and succeeding only if none of the subsystems fail.

The earliest example of a possible application in defense was the suggestion to interpret an aircraft carrier's flight deck operations as an O-ring production function.[3] That is, unless everything falls into place, catastrophic failure may result, as the USS Forrestal accident on July 29, 1967 sadly demonstrated. An example of an O-ring-like sequence, though not in name, is provided in the book Naval Operations Analysis. It states that for a submarine to succeed in destroying an enemy submarine, it would first have to detect it, then identify it as the correct target, work out a firing solution, launch the torpedo(es), at least one torpedo would have to make contact with the target, not become fooled by any decoys, and its exploder should eventually fire the warhead.[4]This sequence illustrates how every other kind of kill chain can also be interpreted as an O-ring production function as well, from the general idea of an OODA loop to the use of a drone strike to take out an indi-

*This article was first published in *Journal of the Americas*, 3, no. 2 (July 2021).

vidual terrorist. It also holds for every individual weapon system, whether a WWII pursuit plane such as the P-40 Warhawk; an M1 Abrams battle tank; or last but not least, the F-35 Lightning II. The concept's very essence carries over to other nonstochastic models where "intelligence," "resources," and "political opportunity structures" are "multiplied, as opposed to summed, to reflect that all components are necessary" to have a chance of winning in unconventional warfare.[5]

The F-35: A State-of-the-Art O-Ring Production Function

Generally considered the most advanced fighter plane in existence, the F-35 not only displays extreme maneuverability and lethality but is a platform incorporating all the subsystems needed to conduct a strike against surface and aerial enemy targets alike. Still, it is an O-ring production function. Sticking with the OODA paradigm, a pilot unable to observe or orient would be unable to decide, let alone act. Thus, if any of an F-35's subsystems are incapacitated—either kinetically, by means of a cyberattack, or just by jamming—the whole platform is basically rendered useless. The mathematics behind the O-ring production function elucidates the dilemma.

The scenario assumes there are four tasks or subsystems needed to successfully complete a mission—such as "observe," "orient," "decide," and "act." The probabilities for these tasks to be successfully met are denoted by p_1, p_2, p_3, and p_4, respectively. The probability of mission success, assuming stochastic independence, is given by $p_1 \cdot p_2 \cdot p_3 \cdot p_4$, and the probability of mission failure by $1 - p_1 \cdot p_2 \cdot p_3 \cdot p_4$. To give a numerical example, even if every subsystem has a 90 percent chance of doing exactly what it is supposed to do, the mission success probability is $(0.9)^4 = 0.6561$; that is, the mission will fail in more than one out of three cases. If the subsystem success rate is increased to 95 percent, the probability of failure would go down to $1 - (0.95)^4 = 0.1855$, but the mission would still fail in almost one in every five cases. One would be mistaken, though, in assuming that increasing a subsystem's reliability is an easy way to alleviate the problem. Prima facie increasing (all) subsystems' reliabilities by 5 percentage points to increase the overall success probability by roughly 24 percent—from 0.6561 to 0.8145—looks a great idea. The cost of increasing any subsystem's reliability is exponential. It would cost less to increase its success probability from say 70 to 80 percent than increasing it from 80 to 90 percent, and the additional cost becomes ever more prohibitive the closer one gets to 100 percent. In terms of the O-ring production function theory and denoting the cost functions by $C_i(p_i)$, this reads as $C_i' > 0$ and $C_i'' > 0$. To illustrate the effect by using the simplest functional form for an O-ring-compatible cost function, $C_i(p_i) = 1/(1 - p_i)$, if a subsystem's reliability were to be raised from 70 to 80 percent, the cost would rise by 50 percent; raising reliability from 70 to 90 percent would triple the cost. Finally, it should be superfluous to point out that a success probability equal to one is impossible to achieve—just as man is not perfect, there are no technologies available that never fail.

From US (Not Only Air) Superiority to Anti-Access/Area Denial

Throughout history and up to and including WWII, warfare has largely been a numbers game. At the beginning of the Pacific War, the *Zero* was the most advanced fighter plane; Japan didn't have enough of them, though. In contrast to their American counterparts, Japanese pilots had combat experience, but again, there were too few. The German *Tiger* was considered the best tank of its time, vastly superior to say the American *Sherman*. Luckily for the Allies, though, there were many more *Shermans* around than *Tigers*.

All of this is in line with (tactical) warfare models. Bradley Fiske in 1905 and Frederick Lanchester in 1916 suggested that, in naval combat and aerial combat respectively, doubling a force's quantity should be more important than doubling its quality. Incidentally, unbeknown to Lanchester, a paper written by Jehu Chase in 1902, when he was a lieutenant at the Naval War College, was a forerunner in describing naval warfare. The mathematics were the same, but Chase, in contrast to Lanchester and Fiske, had even taken staying power such as defensive characteristics into account. Using his model, Chase pointed out the advantages of the tactics of isolating enemy forces. This recommendation led immediately to the paper being classified. It was not declassified until 1972.[6]

From the end of WWII and through the Cold War decades, however, the picture changed as the US attained an ever-expanding gap in weapon technology advances over its peer rivals, Russia and China. The simple reason was economics. Just as a command economy could not compete with a free-market economy, neither could its defense industrial base. Russian numerical superiority did not help. The higher kill ratio of US weapon systems would have sufficed to halt Russian forces. Russian submarines could be tracked wherever they went, but not vice versa, and Russian commanders knew this. Precision bombing during the Vietnam War saw the advent of the "one bomb, one target" capability. US air superiority achieved its heyday during Operation Desert Storm. US stealth fighter-bombers could enter Iraqi airspace at will, and as General David Deptula noted in 2001, "The Gulf War began with more targets in one day's attack plan than the total number of targets hit by the entire Eighth Air Force in all of 1942 and 1943—more separate target air attacks in 24 hours than ever before in the history of warfare."[7]

The picture changed with 9/11 and the ensuing wars in Afghanistan and Iraq for three reasons. First, top-of-the-line air combat platforms were no longer considered necessary for counterinsurgency operations. Second, the cost of fighting two wars at the same time pushed back other expenditures, leading to a reduction in the numbers of F-22s and F-35s. Third, airspace was implicitly assumed to continue being uncontested. However, having had ample opportunities to study the American way of war over the decades US forces had reigned supreme, Russia and China—aware that they would remain unable to match US technological developments and military expenditure—chose to take an altogether different path. Rather than trying to play catch-up, they changed the game by embarking on doctrinal responses and strategies that would render US forces' superiority useless. The two countries would simply bar access to disputed areas, such as the Baltic Sea or the South China Sea respectively, and/or deny the ability to operate in those areas (i.e., A2/AD). In particular, by area denial, US operations in the respective area would be impeded or slowed down at best, effectively preventing US forces from pursuing the fundamental principle of tactical warfare which is, as the US Navy puts it, "Fire effectively first!"[8] Any attempt to enter the contested battlespace would be met by a both fierce and relatively cheap resistance. The cost of a Chinese DF-26 "carrier-killer" anti-ship missile comes at a fraction of any of its intended targets—it would make US losses unsustainable.

The outlook is bleak. War games keep proving that Chinese forces, by embarking on what Jeffrey Engstrom calls a "system confrontation" strategy and by conducting "system destruction warfare," would win against even the most advanced weapon systems, such as the F-35.[9] The basic elements of "system destruction" are attacking the joints, or nodes, by disrupting an adversary's flow; targeting networks and data links (thereby isolating his forces); targeting an adversary's high-value assets by disabling their essential elements (such as C2, ISR, and/or other essential subsystems); disabling an adversary's operational infrastructure; and slowing down an adversary's kill chains. To quote from the final report of the National Defense Strategy Commission:

> If the United States had to fight Russia in a Baltic contingency or China in a war over Taiwan . . . Americans could face a decisive military defeat. These two nations possess precision-strike capabilities, integrated air defenses, cruise and ballistic missiles, advanced cyberwarfare and anti-satellite capabilities, significant air and naval forces, and nuclear weapons—a suite of advanced capabilities heretofore possessed only by the United States. The U.S. military would face daunting challenges in establishing air superiority or sea control and retaking territory lost

> early in a conflict. Against an enemy equipped with advanced anti-access/area denial capabilities, attrition of U.S. capital assets—ships, planes, tanks—could be enormous. The prolonged, deliberate buildup of overwhelming force in theater that has traditionally been the hallmark of American expeditionary warfare would be vastly more difficult and costly, if it were possible at all. Put bluntly, the U.S. military could lose the next state-versus-state war it fights.[10]

Cutting the number of US platforms—whether they are B2s, F-22s, or F-35s—certainly didn't help, nor does the fact that they are O-ring production functions.

Mosaic Warfare

"Mosaic warfare" is a brainchild of the Defense Advanced Research Projects Agency (DARPA).[11] With the publications of the Mitchell Institute's research study authored by Deptula and Heather Penney[12] and a shortened version in *Air Force Magazine*,[13] the idea has entered military mainstream discussions.

The basic idea of mosaic warfare is amazingly straightforward and intuitively striking. If your adversary goes after your systems—"system destruction warfare"—just disaggregate your systems! Rather than putting all proverbial eggs (read subsystems or nodes) in one basket (read on board a single [O-ring production function] platform such as the F-35), use small platforms hosting disaggregated nodes instead. If your original force consisted of say four F-35s, opt for four small platforms hosting only one node each of the kill chain, say observation; opt for four small platforms hosting just another node of the kill chain, say orientation; and so on. And make sure every small platform can independently communicate with every other platform. If just one small platform were disabled, there would be no harm whatsoever because the remaining three platforms hosting the same subsystem or node would take over. In contrast, disabling one F-35's subsystem or node would render that F-35 ineffective. If every F-35 took just one hit, there would be no kill chain left. On the other hand, rendering a disaggregated kill chain network inoperable would require disabling not just any four small platforms but four identical platforms (i.e., all those hosting the same node). While the effect of this strategy is obvious—the probability of mission success should increase with mosaic warfare—its magnitude is not.

Some Mosaic Warfare Mathematics

To illustrate the extent of the benefits to be expected when switching to mosaic warfare, consider an F-35's kill chain consisting of k nodes—using the OODA loop picture, k would equal four—and having an n-ship formation. Assume that for the mission to be successful, it would suffice if just one ship gets through and delivers the kill. Then, using the same notation as in the F-35 section, the probability for an individual F-35 to get through would be $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ and the probability of failing or having to abort, correspondingly, would be $1 - p_1 \cdot p_2 \cdot \ldots \cdot p_k$. With stochastic independence, the most likely scenario, the probability for all n ships to fail would be $(1 - p_1 \cdot p_2 \cdot \ldots \cdot p_k)^n$. Therefore, the probability of successfully completing a mission when using n F-35s (i.e., having at least one ship survive to deliver the kill) is

$$(1)\ \text{prob}\ (\text{success}|\text{F-35s}) = 1 - (1 - p_1 \cdot p_2 \cdot \ldots \cdot p_k)^n.$$

Alternatively, assume that instead of having all k nodes hosted by one (F-35) platform, k small subplatforms are used for every F-35, each of which is responsible for just one of the k nodes. Then any of the k nodes would be compromised only if all its respective n subplatforms are destroyed or rendered ineffective by other means. To isolate the mosaic warfare effect, all p_1 through p_k are assumed to remain unchanged (most likely at least some of these probabilities would go up, as subplatforms should be harder to detect due to being smaller; some subplatforms could also be unmanned, increasing their maneuverability). Then, as the probability of node i to fail equals $(1 - p_i)^n$ the probability of node i surviving is $1 - (1 - p_i)^n$, and the probability of all nodes surviving and of mission success therefore is

$$(2)\ \text{prob}\ (\text{success}|\text{mosaic warfare}) = (1 - (1 - p_1)^n) \cdot (1 - (1 - p_2)^n) \cdot \ldots \cdot (1 - (1 - p_k)^n).$$

The difference between (2) and (1) gives the increase in the chances of mission success due to switching to mosaic warfare.

To visualize the magnitude of the influence of mosaic warfare, assume that all p_i are identical, henceforth denoted by $p := p_1 = p_2 = \cdots = p_k$.[14] Then (1) and (2), respectively, can be simplified to

$$(1a)\ \ \text{prob}\ (\text{success}|\text{F-35s}) = 1 - (1 - p^k)^n \text{ and (2) becomes}$$
$$(2a)\ \ \text{prob}\ (\text{success}|\text{mosaic warfare}) = (1 - (1 - p)^n)^k.$$

This formula allows for evaluating the outcome of different scenarios by means of a simple pocket calculator.

It is obvious that for any one-ship mission there cannot be a mosaic warfare effect. Therefore, assume n = 2 (i.e., a two-ship mission) and k = 4 (OODA). With p = 0.9, (1a) yields 0.88173279, while (2a) yields 0.96059601 (i.e., switching to mosaic warfare would improve the chances of mission success by about 7.9 percentage points). However, as an F-35 mission success probability of around 88 percent still sounds pretty good and is not exactly in line with "the U.S. military could lose the next state-versus-state war it fights",[15] try p = 0.7 instead. (1a) would yield 0.42255199 – now the mission would fail more often than not – while (2a) would yield 0.68574961, i.e., mosaic warfare would increase the chance of winning by about 26.3 percentage points and raise it above the two-out-of-three level.[16]

Formulae (1a) and (2a) can be used to easily evaluate the outcomes of other scenarios by toying with k, n, and p (i.e., whether it is a change in the number of subsystems or nodes, the number of platforms, or the reliability of the subsystems). The results stay true: mosaic warfare will always improve the chances of mission success, and the more even the odds of an F-35 mission being successful, the higher the benefits to be gained.

Summary

This article was never intended to prove the validity of the mosaic warfare concept. Particularly, it did not even try to address technological or doctrinal questions such as the danger of communications between subplatforms being compromised (mission failure would be obvious; on the other hand, should an F-35 become isolated, it could still try to proceed). Neither did it address how long it would take to develop subplatforms and bring them into service (the South China Sea conflict could turn hot any time soon); the time it takes to devise a new doctrine (as long as the commander in the field remains unconvinced, all is in vain); or the compatibility of "traditional" air war (i.e., putting one's trust in highly sophisticated but more vulnerable O-ring production function weapon systems) and applying mosaic warfare (can they be run in parallel?).

That said, for any new idea to live on, the word must get out; the story, including every single facet, has to be circulated. This article concentrates on the likely magnitude of the mosaic warfare effect on mission success. Using a not-exactly-rocket-science mathematical argument, the article suggests that this approach can, more often than not, substantially improve the chances of mission success in scenarios where traditional approaches are bound to fail. Considering that mosaic warfare systems can come a lot cheaper than the single-platform weapon systems in use today, mosaic warfare could begin to look ever more attractive. ✪

Jörg Schimmelpfennig

Dr. Schimmelpfennig, emeritus professor of theoretical and applied microeconomics at Ruhr University, Bochum, Germany, is a member of, inter alia, the Royal United Services Institute, Institute for Defense and Government Advancement, the US Naval Institute, the Naval Historical Foundation, the Army Historical Foundation, the Air Force Association, and the Army Records Society.

Notes

[1] *Report of the PRESIDENTIAL COMMISSION on the Space Shuttle Challenger Accident*, NASA (website), 40, https://history.nasa.gov/.

[2] Michael Kremer, "The O-Ring Theory of Economic Development," *Quarterly Journal of Economics* 108, no. 3 (August 1993): 551–75.

[3] Gene Rochlin, Todd La Porte, and Karlene Roberts, "The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea," *Naval War College Review* 40, no. 4 (1987): 76–90.

[4] Daniel H. Wagner, W. Charles Mylander, and Thomas J. Sanders, eds., *Naval Operations Analysis* (Annapolis, MD: Naval Institute Press, 1999).

[5] William "Dave" Driver and Bruce E. DeFeyter, *The Theory of Unconventional Warfare: Win, Lose, and Draw* (Monterey, CA: Naval Postgraduate School, 2008).

[6] Bradley A. Fiske, "American Naval Policy," *Proceedings of the United States Institute 31* (January 1905): 1-80; Frederick W. Lanchester, *Aircraft in Warfare: The Dawn of the Fourth Arm* (London: Constable, 1916); and Jehu V. Chase, "A Mathematical Investigation of the Effect and Superiority of Force in Combats upon the Sea," (unpublished paper, Naval War College Archives, Newport, RI, [1902]).

[7] David A. Deptula, *Effects-Based Operations: Change in the Nature of Warfare* (Arlington, VA: Aerospace Education Foundation, 2001).

[8] See Wayne P. Hughes, *Fleet Tactics and Coastal Combat*, 2nd ed. (Annapolis, MD: Naval Institute Press, 2000).

[9] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND Corporation, 2018).

[10] Eric Edelman and Gary Roughead, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Washington, DC: United States Institute of Peace, 2018): 14.

[11] DARPA, *Strategic Technology Office Outlines Vision for Mosaic Warfare* (DARPA, August 4, 2017, https://www.darpa.mil/).

[12] David A. Deptula and Heather Penney, *Restoring America's Military Competitiveness: Mosaic Warfare* (Arlington VA: The Mitchell Institute for Aerospace Studies, 2019).

[13] David A. Deptula and Heather Penney, "Mosaic Warfare," *Air Force Magazine* 102, no. 11 (2019): 51–55.

[14] If the sub-systems' cost functions are identical, $p_1 = p_2 = \cdots = p_k$ would be the cost minimizing/success maximizing solution anyway.

[15] Edelman and Roughead, *Providing for the Common Defense.*

[16] It should be noted, though, that if was reduced further, the gain, while always being positive, will eventually become smaller again.

All the Factors of Victory: Adm. Joseph Mason Reeves and the Origins of Carrier Airpower by Thomas Wildenberg. Naval Institute Press, 2019, 352 pp.

Thomas Wildenberg, an independent historian specializing in the development of US Navy aviation and technological innovation, argues Admiral Joseph Mason Reeves is an unsung hero by offering his progenitor role in the development of carrier aviation operations, tactics, and employment during the interwar years as evidence.

In *All the Factors of Victory: Adm Joseph Mason Reeves and the Origins of Carrier Airpower*, Wildenberg elects a biographical perspective tracking Reeves's life from childhood to death. Unfortunately, Wildenberg's effort is hampered by one rather difficult problem: there is not much written or documented about the life of Admiral Reeves. This problem forces Wildenberg, by his admission, to "borrow generously" from a single-source document, a doctoral thesis titled "Admiral with Wings" and authored by the son of one of Reeves's former chiefs of staff (p. x).

Despite the documentation disadvantages saddling Wildenberg, he produces an easy-to-follow text of Reeves's career populated with occasional leadership lessons suiting the purpose of a biography. The book opens by recalling the pivotal point in Reeves's career where he excelled during Fleet Problem IX, the first annual training exercise that focused on carrier employment.

Wildenberg then shifts back to Reeves's acceptance to the US Naval Academy and sequentially documents Reeves's life until it ends three months after his final retirement from naval service. The effort spends little time on Reeves's personal life, only inferring that his devotion to the sea led to a lonely existence and estrangement from his wife.

Reeves's career was somewhat of an exception in the current era of officer development. He demonstrated an extraordinary aptitude for leadership and innovation in various company- and field-grade officer assignments. He was placed in charge of what was essentially carrier aviation operational testing and evaluation and was given command of the first operational carrier force.

Along the way, Reeves made more friends than enemies and remained cognizant of the other interest groups holding sway—the battleship mafia known colloquially as the gun club. Although somewhat an over-simplification of Reeves's long and impactful career, Wildenberg uses Reeves's successful navigation of these waters as justification for his deserved remembrance.

Any qualms about Wildenberg's effort would be that throughout the biography, the author weighs Reeves's contributions to the propelling of carrier aviation a bit heavier than is warranted. There were many supporters of carrier aviation at all levels during Reeves's career, meaning that the bureaucratic and organizational battles he fought were the ones that often landed on sympathetic ears as many saw the carrier as a mobile air base solution in the vast Pacific for deterring Japanese attacks.

Wildenberg also sporadically uses conjecture to link Reeves's presence in different situations to associated responsibility for follow-on actions, likely driven by the lack of documentation of Reeves's life.

Wildenberg finishes his preface by offering, "As was the case with so many of the exceptional leaders produced by the Navy in the first half of the twentieth century, Reeves was an extremely talented, multifaceted officer whose career stands as a mute tribute to the Navy's leadership during the interwar years" (p. xi).

Admiral Joseph Mason Reeves is not the first great leader whose contributions have been muted by the momentum of time, nor will he be the last. Still, Wildenberg did all that was possible to rescue Reeves from a fate of obscurity. In doing so, he also augments the knowledge of airpower development for aviation enthusiasts and historians focused on the interwar era.

Colonel William J. Ott, USAF, Retired

Bombs without Boots: The Limits of Airpower by Anthony M. Schinella. Brookings Institute Press, 2019, 391 pp.

Bombs without Boots is a timely study of modern airpower, its ability to coerce, and its uses and shortfalls. Anthony M. Schinella, a National Intelligence Council national intelligence officer, brings 25 years of experience to bear while examining five post-Cold War conflicts that saw Western militaries rely heavily on airpower to achieve various objectives. The result is a mix of history and strategy that significantly adds to the debate of airpower capabilities and limitations.

The book delves into Operation Allied Force in Bosnia and Kosovo, the opening months of Operation Enduring Freedom in Afghanistan, Israeli actions in Lebanon in 2006, and Operation Odyssey Dawn in Libya to see how well the modern Air Force succeeds in achieving military and political aims. He quickly explains and demonstrates that the level of success depends significantly on whether the respective military is willing to commit ground troops to a campaign, or, barring that, if there are capable proxies available to fight on the ground and then secure the peace afterward.

The result is a compelling argument of how airpower rarely works well in a vacuum, and that proper ground forces and airpower serve a symbiotic relationship where each strengthens the other's attributes. In the end, Schinella lays out a list of six criteria that military leaders and policy makers should consider before starting a war that will rely on airpower and the use of proxy forces. His list is not exhaustive but serves as a good starting point for discussion.

The book is a useful contribution to airpower strategy, but it does have limits. The case studies involved are useful for determining air strategy for small wars against less capable enemies. There is little discussion of what to do in situations where enemy forces have safe havens to retreat and regroup, an often noted problem for airpower during Korea, Vietnam, and Afghanistan after 2002.

Also, the strategy may not serve well when considering actions directly against a peer adversary. While these topics may be beyond the scope of the author's original study, they deserve consideration when determining the efficacy of airpower.

That being said, operational and strategic air planners should pick up a copy of *Bombs without Boots*. It goes a long way toward understanding the conflicts covered in the case studies and can add significant insight into a potential conflict in current hotspots like Iran or Venezuela. There is definitely room in the ever-changing airpower debate for Schinella's ideas.

Major Ian S. Bertram, USAF

Middle East 101: A Beginner's Guide for Deployers, Travelers, and Concerned Citizens by Youssef H. Aboul-Enein and Joseph T. Stanik. Naval Institute Press, 2019, 422 pp.

While *Middle East 101: A Beginner's Guide for Deployers, Travelers, and Concerned Citizens* is touted as a beginner's guide, it provides an engaging, comprehensive overview of Middle Eastern political and religious history. Beginning in southern Mesopotamia in 5,000 BC, Youssef H. Aboul-Enein and Joseph T. Stanik recount the formation of Islam, the internal and external conflicts plaguing many areas of the Middle East throughout history, and the subsequent perversion of sharia law by small groups of extremist, militant jihadis.

Where *Middle East 101* proves to be a beginner's guide is in the sense that no prerequisite knowledge is required to follow the authors' explanation since background knowledge is provided, and everything is laid out in an organized, chronological fashion. Aboul-Enein is a US

Navy commander and Middle Eastern Studies scholar who has authored many books. Stanik is a retired US Naval officer and history teacher who has published works as well. The authors' credentials shine through in this work as they can take a complex subject and make it reasonably simple to understand.

The book is mostly expository, and the authors remain unbiased in their descriptions of events. One of the only opinions implicitly posed is that there is a need for Western society—service members especially—to build a deeper understanding of the history that defines the relationships between different Middle Eastern countries and Islamic sects, how history has shaped the region's attitudes toward us, and how these relationships influence our US foreign policy.

History tells us that a lack of information and understanding often leads to prejudice. The authors themselves mention, "we must not alienate through prejudice or fear-mongering the very population whose help is needed to counter militant Islamist ideology and watch for militant Islamist cells forming in our communities. We are assuredly not at war with Islam." (p. 367). It is indeed unfortunate that the average American war fighter knows so little about people whose lives have become so intermingled with ours, as our actions in that region and attitudes toward Muslims, both at home and abroad, affect them in a profound way.

While they served the purpose of laying the ground for later chapters, there are some early sections in this book that are a little difficult to keep up with due to the depth of information. The Middle East is an ancient and diverse region, which understandably makes it difficult to summarize its history without including a high degree of detail.

Every service member and American citizen could benefit from reading *Middle East 101*. It would even be appropriate for a condensed version of this work or its themes and overarching message to be a part of various services' military induction training curriculum because it would provide Airmen, Marines, Sailors, Soldiers, and Guardians a lens through which to view the region and gain a deeper understanding of what we fight for.

Senior Airman Kyle K. Stiff, USAF

Beyond Blue Skies: The Rocket Plane Programs That Led to the Space Age by Chris Petty. University of Nebraska Press, 2020, 408 pp.

Chris Petty is a space and aviation enthusiast and author of The High Frontier blog. *Beyond Blue Skies* is his first major book, focused on the high-speed research aircraft programs conducted by the National Advisory Committee for Aeronautics (NACA, later NASA), the Air Force, and the Navy from the end of World War II through the mid-1970s.

Encounters with transonic compressibility in fighter aircraft and the advent of jet propulsion focused post–World War II aeronautical research on issues associated with flight near to and faster than the speed of sound: the legendary "sound barrier." As contemporary jet engines lacked the performance to sustain such speeds, NACA researchers proposed using rocket-propelled aircraft to explore supersonic flight until jet power caught up. The Air Force, influenced by Theodore von Kármán's *Toward New Horizons* report—and to a lesser extent, the Navy—became enthusiastic partners, and an era of high-speed flight research bloomed above the California desert.

Petty adroitly captures the tension between the services seeking to demonstrate US aeronautical primacy through speed and altitude records, the NACA's less dramatic goals of painstakingly expanding the understanding of transonic and supersonic aerodynamics, and later support to the evolving NASA and Air Force manned spaceflight programs. He also strikes a balance between the technical aspects of different experimental programs and the human aspects, particularly the small group of individuals involved across the 30-year period.

The book leans heavily on previously published material, something that Petty highlights in his introduction, noting tongue-in-cheek that he should have written this book 20 years ago when more of the individuals involved were still available to interview. Nevertheless, Petty's research is comprehensive, extending across official NASA and service reports, archived interviews and memoirs published by test pilots and engineers, and news media coverage of key events.

While Petty's book doesn't break much new ground, it combines material from a wide variety of sources into a highly readable, one-volume history of an important and inspiring period in US aviation history. It is a highly recommended read.

Colonel Jamie Sculerati, USAF, Retired

Save Your Ammo: Working across Cultures for National Security by Louise Rasmussen and Winston Sieck. Global Cognition, 2019, 255 pp.

Why is cultural education important for everyone? *Save Your Ammo* is a book that provides the answer. Louise Rasmussen and Winston Sieck, founders of Global Cognition, compile an engaging, entertaining, and instructive collection of vignettes that highlight the importance of cultural savvy in global military missions.

Rasmussen and Sieck's credibility as scholars is impeccable on its own merits; their instantly eye-catching book has several noteworthy professionals providing endorsements. General Anthony Zinni, USMC, retired, former US Central Command commander, and Major General Michael Rothstein, USAF, retired, former Air University vice commander and Curtis E. LeMay Center for Doctrine Development and Education commander, are just two of the endorsers whose words validate the accuracy and utility of the material for readers.

If the goal of *Save Your Ammo* is to make culture accessible and practical for the personnel engaging with their international counterparts, the intent is successfully achieved. The target audience is personnel who will engage their allied or coalition counterparts likely below the diplomatic level. Content at the practitioner level is sometimes presented as prescriptive dos and don'ts, giving the impression that culture is a one-size-fits-all proposition.

But *Save Your Ammo* is a welcomed departure—nuanced but simple. Readers of Malcolm Gladwell or Chip and Dan Heath will feel right at home with the authors' style of introducing a topic, sharing and explaining extraordinary experiences of ordinary people, and leaving readers with practical lessons at the end of the chapter.

From the opening vignette of a Marine's tense engagement with a warlord in West Africa, the folksy style of storytelling pulls readers into the pages and places them in the boots of the story's subject. Through the eyes and the direct words of those extensively interviewed individuals, readers will learn and experience the lessons of those who got it right, those who did not, and those who discovered the importance of lifelong learning.

In addition to the high-quality storytelling, another strength of the book is the clarity of the lessons. Being well-defined in the chapter text and succinctly bulleted at the end of the chapter, the authors make clear what they want readers to learn—they illustrate those lessons and effectively summarize them to solidify understanding. A great example of a lesson on perspective can be found in the vignette of Air Force Captain Muñez. He learned from an Afghan elder that there are differences in warrior culture between American military members and Afghan counterparts (pp. 97–99). That lesson helped him understand tactics and decision-making, enhancing interoperability during his deployment.

The complimentary vignettes of Marine Corps Colonel Hanson (pp. 67–68) and Army Staff Sergeant Aaronson (p. 68) effectively communicate the importance of continuous learning in a combination of a "course and experience." Especially compelling is the story of Air Force Senior Master Sergeant Krautkremer and his unique experience in Kazakhstan (pp. 158–61). There is an important lesson in trying to get a civil engineering project complete when cultural perspectives collide on the prioritization of tasks. Understanding the perspective of culture from those who were there long before and those who will be there long after redeployment is a sage lesson for all personnel to learn.

One area where the book could be slightly better is when the authors try to do a little too much. There is no shortage of personnel interviewed and cited to illustrate points, and many well-developed vignettes are highly memorable. Others who immediately piqued the curiosity of the reader ended with just a quote. As a result, readers could be left wanting or trying to figure out how a particular input fits into the larger narrative. While this area could have been better, it was not a distraction nor did it detract from overall readability.

Save Your Ammo is an excellent book that should be on the shelf of practitioners. It should be used by academics to supply stories that bring theory to life, and it would make great required reading for anyone before a first overseas deployment. The book reminds us that for all the differences in cultures, there are just as many commonalities that can help establish trust relationships at the tactical and strategic levels. It also reminds us interoperability begins with one human being willing and able to connect with another.

Save Your Ammo would have saved my pride the first time I went overseas many decades ago! I encourage you to read this book and through the vignettes, find your own words to communicate and practice the great power of culture.

Colonel Walter H. Ward Jr., USAF, Retired

Winning Wars: The Enduring Nature and Changing Character of Victory from Antiquity to the 21st Century by Matthias Strohn. Casemate Publishers, 2020, 315 pp.

"So, what is winning?" This is the question posed by Andrew Sharpe in the final chapter of *Winning Wars*, and it is a question that the book seeks to answer through its expansive examination of global conflicts. This collection of essays written by veterans and academics synthesizes various perspectives on war fighting since antiquity. The opening chapters feature a historical analysis of ancient Greece and Rome, the Middle Ages, the Early Modern Period, and the Napoleonic Era. This analysis is followed by an evaluation of contemporary conflicts and cultural traditions that encapsulate victory in warfare. These chapters encompass the World Wars, the Cold War, The Troubles, Iraq, Afghanistan, Syria, and several other examples of modern conflict, as well as cultural perspectives from Russia, China, and Iran.

The book was published for the Centre for Historical Analysis and Conflict Research, and the 18 contributors include published authors in the field. Because each chapter focuses on a specific historical period, culture, or modern conflict and is written by an expert in that subject, the reader is provided with an extensive historical and cultural context from which to analyze the armed conflicts of today. Needless to say, *Winning Wars* is not limited to history as it incorporates elements of international relations and cultural anthropology in ways that complement its contribution to the field of military science.

As one might expect, the authors do not settle on a permanent, uninterrupted definition of what "winning" means. This is largely because this definition has changed rapidly over time. As such, the authors find themselves discussing winning (as opposed to defining winning) because a contemporary understanding of winning is, in some cases, very different from what it has looked like in times and places past. This is of great interest to all of those who currently serve, however, as we enter our twentieth year in Afghanistan. As John France writes in the second chapter, our recent conflicts such as Iraq and Afghanistan "represent something more like the experience of Europe in the Middle Ages—worlds in which war is a norm and winning is hard to define" (p. 44).

Due to the academic nature of the book, the contributors stay away from making political pronouncements regarding current military engagements. But they do offer policy recommendations beyond the typical condemnation of mission creep or criticism of short-sighted US strategy in Iraq and Afghanistan. For example, they highlight the reluctance in Washington to account for and adapt to strategic goals that changed over time, recommending policy makers "expect goals to change" in modern asymmetrical conflict (p. 144).

They point to inconsistent communication between senior members of the armed forces and the civilian leadership that persisted for years, quoting senior officers who were openly skeptical of policy to other officers, but never relayed strategic concerns to policy makers. The authors recommend a "robust dialogue between civilian and military leaders" to facilitate adequate forethought and preparation for a wide range of possible military outcomes and to solidify coherent and achievable military objectives (p. 144).

These foreign policy interests of policy makers should be considered against the potential risks and costs of an intervention, and the authors are clear that the probability of issues such as mission creep is a viable reason to avoid entanglements altogether. Given the current status of these conflicts and assessing the numerous risks that were unaccounted for at the outset of these conflicts, the authors are abundantly forthright in their counsel, "Staying out of wars is usually the best strategy of all, if one cannot define national interests" (p. 145).

In total, the book is ambitious; each chapter could be a full-length book in and of itself. But the authors succeed at presenting a wide range of information in a way that is easily digestible and relevant to the overall analysis. Every chapter offered a comprehensive assessment of a complex subject matter that could be used to complement further inquiry into military strategy and policy making. For example, chapter 9, by Richard Kuno, presented one of the most thorough and clear-sighted analyses of the Syrian Civil War that is available for public consumption. Chapter 11, by Kerry Brown, offers insight into the historical and cultural factors that influence actions we see from China's leadership today.

The authors show how ambiguous definitions of winning have impacted conflicts from ancient Rome to Northern Ireland and even South Sudan. Due to the multitude of contributors, the book provides a unique insight into a wide variety of subjects without feeling overly condensed or rushed. It can provide useful insights to anyone; students and subject matter experts alike can find something to gain from this book. Most importantly, its emphasis on contemporary warfare can provide consequential information for our current military and civilian leadership, if they are willing to hear it. As such, the lessons from *Winning Wars* should be taken to heart as we assess our position in conflicts around the globe.

2nd Lieutenant Micah Mudlaff, USAF

Defense Engagement since 1900: Global Lessons in Soft Power edited by Greg Kennedy. Kansas University Press, 2020, 312 pp.

In the middle of the Department of Defense's shift from wars in the Middle East with extremist groups to power struggles with near-peer adversaries, new strategic centers of gravity come into focus, chief among them, soft power. In no other way can the United States retain allies and keep intact its sphere of influence over nations near to China and Russia.

In this context, *Defense Engagement since 1900* is an ambitious work of applied military history meant for all readers, but particularly those focusing on military and political affairs. The book offers lessons from the past for current challenges through 10 case studies by different authors. The collection is compiled and introduced by Greg Kennedy, a professor in the Defence Studies Department at King's College London.

The United Kingdom's (UK) International Defence Engagement Strategy defines defense engagement (DE) as "the use of our people and assets to prevent conflict, build stability, and gain influence" (p. 243). Throughout the course of the book, Kennedy and the other authors put forth various considerations to support embracing defense engagement in the UK and abroad. Notably, the case study is a unique form of analysis that furthers military and political research by comparing a historical analysis to contemporary defense problems. While the vehicle of a case study may risk losing some readers, Kennedy uses it well by placing current policy issues alongside historical lessons learned.

Defense engagement is not a new concept, but its applications are continually refreshed. It embodies the desire to achieve influence and advantage by "engaging with neutral nations, allied nations, and even adversarial nations through military interactions" (p. 2). Such interactions are not simply kinetic in nature; instead, the intention is to utilize soft-power attributes within the military power sphere.

These activities and actions run the gamut from "war-gaming, exercising, and common-doctrine creation through to technological exchanges, professional military education, and intelligence sharing" (p. 3). Ultimately, the aim of DE is akin to the aim of alliance building: to deter, assure, attract, and prevent. Deterring wars is better than winning wars in the first place.

Defense engagement was first espoused as a British military activity in the *National Security Strategy* of 2010 to tackle risks before they escalated. This engagement is historically championed by military attachés—officers who commonly straddle the military and diplomatic divide. Attachés are uniquely positioned to examine the ability of a state's military to move away from thinking of its role as the applicator of force and toward an applicator of power. The DE *influence* is at the core of what this application of military power aspires to accomplish.

Of the book's 10 case studies, the most contemporary is the final one concerning the Brexit decision, Britain's new position in the world, and DE's ability to ameliorate some of the undesired ramifications of Brexit. By not viewing Britain through the lens of a "Remainer" or "Brexiteer" but rather through the lens of the United Nations, the authors find evidence for a decline in the UK's world standing following the Brexit decision. Immediately after Brexit, for example, the UK suffered a 15 percent devaluation of its currency.

Brexit's peculiar harm to defense strategy was the utter lack of clarity on where the government's priorities lie. Did the UK wish to remain a global nation with global influence, or should it seek to focus more on Europe? There were no easy answers to these questions, causing further tension within the government. Regardless of whether one sees Brexit as a golden opportunity or a looming threat, the decision taken by the UK public on June 24, 2016 appears to have taken some toll on the UK's international standing.

The authors of the Brexit case study make clear that DE can help mitigate some of the negative effects of the UK's departure from the EU. They state that a renewed focus on the enduring UK-US relationship is more vital than ever. Also, a clearer focus on European engagement through existing institutions such as NATO offers the advantage of efficiently reaching 28 nations through a single aperture. The UK's military can next pay particular focus on its closest European Allies—France and Germany—with a close second priority on the near-abroad. Ultimately, an "everything everywhere" approach will clearly not deliver the desired outcomes, so the authors propose it is time to rethink the scale of the UK Defence Department's contribution to the country's international ambition.

Be forewarned that the scope of *Defense Engagement since 1900* is narrow. It puts forth a perspective focused on the UK and is primarily European in scope. While parallels can be drawn to other nations and conflicts, one should know in advance that the book ultimately targets a Eurocentric audience.

A second critique is that not all the chapters offer true case studies in DE. The first chapter, for example, is primarily a historical recounting of the military attaché roles in various European countries from 1900–19. This recounting is a case study only in the loosest sense; it is better categorized as a historical summary. Finally, each chapter features another author's voice and approach; some are dusty and didactic, while others sparkle with the author's wit and personality.

Defense engagement will surely grow in popularity in the UK and abroad. The Department of Defense recently released the unclassified portion of the *Irregular Warfare* Annex to the *2018 National Defense Strategy*. Thus it is clear the American military also values scholarship on the topic of influence and legitimacy among foreign populations. In the end, the book predicts several leading militaries must take on unconventional roles in the United Nations and NATO, recasting themselves in the coming years from wielders of force to employers of power.

Captain Matthew H. Ormsbee, USAF

Handprints on Hubble: An Astronaut's Story of Innovation by Kathryn D. Sullivan. MIT Press, 2019, 304 pp.

At first glance, a spacewalk (called an extravehicular activity or EVA in the acronym-laden jargon of the National Aeronautics and Space Administration [NASA]) seems cool, fun, and—after hundreds of them carried out during the past 55 years—routine.

In reality, they are anything but a lark. Space is an exceptionally dangerous and harsh environment; several astronauts and cosmonauts have come much closer to perishing on EVAs than is commonly known. The spacesuits are actually miniature human-shaped spacecraft with all the complexities that implies. Astronauts find it difficult to work in them, and wearing a spacesuit can range from uncomfortable to downright painful for the occupant. The fact that EVAs can be done at all is impressive; that they can be done safely while highly exacting work can be accomplished is the result of diligent and brilliant engineering.

Kathryn D. Sullivan was a young oceanographer when NASA selected her to become an astronaut in 1978. Sullivan, from the first class of astronauts selected after the Apollo program, was one of the first American women included in the famed Thirty-Five New Guys. Part of the book is Sullivan's memoir of her application, selection, and training to become an astronaut, and her shuttle flights. But much of the book describes the efforts of the team, which included Sullivan, to develop an on-orbit maintenance capability for the Hubble Space Telescope.

The Hubble Space Telescope has been described as the most productive scientific instrument in history. Sized to fit in the cargo bay of the space shuttle orbiter, Hubble is a large optical telescope designed to make astronomical observations that are unimpeded by Earth's atmosphere, which can distort and block electromagnetic radiation received from planetary and celestial bodies.

Before Hubble, scientific satellites had been launched and would never be touched thereafter, which meant they could not be maintained, repaired, or upgraded. In contrast, Hubble was designed to be visited periodically by the space shuttle and serviced by astronauts on EVAs. Not only was Hubble intended to be an important astronomical tool, but it was also a flagship mission for the space shuttle, showing the value of a reusable spacecraft with a human crew.

Conceptually, the marriage of the space shuttle and Hubble made sense. Translating from concept to implementation is an enormously challenging project, and that journey is the heart of Sullivan's book.

What parts of Hubble should be serviceable? How should Hubble be designed and built to enable its servicing? What tools are needed? What procedures? How can all these things be made compatible with the limitations imposed by EVA including items such as bulky space suit gloves? How can the astronauts use these tools and execute these procedures safely? How can Hubble's design, tools, and procedures, all intended to be used in the almost airless microgravity environment of space, be tested and validated on the ground? All these concerns were uncharted territory in which invention would be needed.

Sullivan does a wonderful job of describing the process of innovation by the Hubble servicing team, which included members from several NASA centers as well as contractors. The reader learns about Sullivan's role but also meets compelling people like Frank Costa, a Lockheed engineer who managed the Hubble's electrical system, and Brian Woodworth, who designed the tools that astronauts would use. Sullivan paints a vivid and admiring portrait of each of these people and many more.

We now know in hindsight what the Hubble in-flight maintenance team could not have known in advance: that Hubble was built with a serious flaw in its optical system that was only discovered after launch and prevented it from accomplishing the intended mission. The capabilities developed by the team did not just enable Hubble to have its service life extended. They were required to save Hubble from almost total failure. Additional servicing missions have greatly improved the observational powers of Hubble and keep it operational as it begins its fourth decade in orbit.

Handprints on Hubble is an outstanding book worth reading. Readers learn about how high-performance teams innovate and how NASA really carries out the marvelous things that it does.

Kenneth P. Katz

Chinese Communist Espionage: An Intelligence Primer by Peter Mattis and Matthew Brazil. Naval Institute Press, 2019, 376 pp.

Chinese Communist Espionage: An Intelligence Primer lifts the veil of the Chinese Communist Party's (CCP) intelligence apparatus. Richly sourced from Chinese language texts, Peter Mattis and Matthew Brazil detail an unprecedented number of historical intelligence figures and foundational myths. Just as understanding Admiral Hyman G. Rickover's role as the father of the US Naval Nuclear Propulsion Program gives key insights into contemporary US Navy submarine culture, an intimate understanding of leaders like Zhou Enlai provides insights into the contemporary CCP intelligence culture.

Chinese Communist Espionage is informative and functional for the US intelligence professional. Mattis and Brazil inform readers on the roles played by CCP intelligence operatives during events more commonly studied by US security professionals like World War II, the Nixon administration's opening of relations with China, China's entrance into the World Trade Organization, and other major world events.

Exposing the roles of past shadow actors outlines potential covert strategies today. Functionally, the book indexes relevant CCP activities. For example, *Chinese Communist Espionage* includes biographical sketches of many CCP intelligence figures and traces the ideological genealogies of contemporary leaders. Tracing master-apprentice relationships provides insights on perspectives and whether an intelligence professional's pedigree will facilitate or hinder ascension.

The book separately catalogs prosecuted cases of espionage. The CCP has systematically conducted multilayer penetration in all sectors of US industry. Cases range from stealing agricultural seeds to F-22 jet engine designs. Aside from the scope and scale of the exfiltration, several other trends exist: many operatives are naturalized US citizens, agents frequently leverage third-party countries to bypass US export control laws, and most convicted cases result in relatively short jail sentences.

The CCP intelligence community invests significant efforts to promulgate its heroic organizational myth while simultaneously manicuring the myths of nemeses like US intelligence agencies. The CCP propaganda arm leverages legacies of foreign intervention in the Opium Wars and modern examples like the 2001 US-Chinese E-P3 incident to develop an archetypical enemy that must be defeated.

Universally believed propaganda proves useful during national emergencies, such as recent efforts by CCP officials to blame the US military for creating the Corona Virus. While the international community recognizes such blatant and baseless propaganda as false, it has a receptive audience among Chinese domestic media outlets.

Despite the extreme preference for using intelligence operations for strategic gain, the CCP intelligence community has a mixed record due to its internal conflict over "Red vs Expert." The CCP's proclivity for using intelligence operations as a strategic lever is classic Sun Tzu, but analysis reveals intelligence cadre must balance ideological purity with effective spy craft. Historically, good spies often found themselves purged after cultivating relationships with assets or speaking the truth too plainly. This culture perpetuates analytical blind spots, and episodic purges frequently remove whole cohorts of experienced professionals.

Despite regular upheaval within the intelligence ranks, intelligence officers have enjoyed disproportionate promotion rates in the People's Liberation Army (PLA). Intelligence officers' ability to contribute to domestic political manipulation makes senior intelligence posts a revolving door between military and internal security intelligence organizations. But the dividing focus between party and military intelligence priorities results in reduced proficiency in military intelligence core competencies. PLA intelligence officers promoted based on domestic political manipulation often lack the expected measure of expertise in conventional military operations.

Chinese society accepts internal spying and authoritarian rule at far greater levels than imaginable in Western culture. The stark contrast between Chinese communism and US individualism is important to understand as the United States observes China's covert surveillance apparatus, heavy internet regulation, and social credit system.

Given the acceptance of these cultural norms, the United States must acknowledge the limited potential for influence campaigns to make a meaningful impact on the CCP's control of the populace. Just like the United States learned from decades of conflict in predominately Muslim countries, exposure to US culture and ideals may not reprogram China's long cultural memory.

The CCP's ability to combine sophisticated technical collection with effective human intelligence operations highlights the efficacy of Sino-intelligence activities today. Since the 1990s, the Chinese government has funded many public-private research initiatives that sowed the seeds of Chinese computer network exploit capabilities and domestically produced infrastructure equipment that led to the "Great Firewall."

Much has been written about the Sino-Russian marriage of convenience and the pairing of Russian military prowess with Chinese money. Mattis and Brazil detail historical Sino-Russian relations, which provides context for analyzing the Sino-Russian partnership within China's modern spy state.

Intelligence reforms by Hu Jintao and Xi Jinping catapulted the technical collection capability to a near-peer status with the United States, but the culture of CCP intelligence services remains starkly political. The "Red versus Expert" dilemma results in difficulty filling "inner-line" billets, which exposes agents to enemy detection and subsequent suspicion from CCP internal police after close contact with the enemy.

As a result, the ranks of the CCP intelligence community are full of ideologues, and intelligence products seek alignment with political ideology vice the pursuit of objective truth. This situation starkly contrasts with Western whistleblower protections that prevent political actors from funneling intelligence resources for domestic political gain.

Luo Ruiqing said, "Enemy intelligence work is like a knife, if used well it can kill the enemy, if used badly it might also injure oneself" (p. 98). China's flagrant use of intelligence and espionage agents offers an opportunity for the United States. Decades of economic benefits from the US-China relationship muffled the warnings of Chinese espionage by the US security apparatus, business market, and working-class factions.

In the post-Coronavirus world where all national economies face economic contraction, however, the United States should recognize the opportunity to redefine redlines for Chinese intelligence and espionage activities. Without revealing sources or methods, US political and business leaders should expose China's aggressive intelligence and espionage campaigns. Explicit recognition of Chinese economic dependencies upon US security and industrial provision will provide the needed strategic levers for negotiation.

Lieutenant Commander James M. Landreth, USN

Spying from the Sky: At the Controls of US Cold War Aerial Intelligence by Robert L. Richardson. Casemate, 2020, 301 pp.

Spying from the Sky: At the Controls of US Cold War Aerial Intelligence is the story of the military career of Colonel William Gregory, USAF, with much of it told in his own words. It is also the story of the post-Korean War US Air Force and the Central Intelligence Agency (CIA) development of the national high-altitude strategic reconnaissance program.

Born in poverty in rural Tennessee, Gregory learned to fly in the pre–World War II Civilian Pilot Training Program while attending college. Joining the US Army Air Forces in 1942, he was a P-38 fighter pilot in the Italian theater with three victories. He left the US Army Air Forces after the war but stayed in the Reserve, flying weekends at nearby Barksdale AFB, Louisiana, while finishing his degree and starting a civilian career.

Recalled during the Korean War, Gregory transitioned to flying B-29s. He was offered a chance to stay in the USAF after the war and accepted without discussing it with his wife. She later discovered this at the Barksdale AFB Officers Club's party, leading to a sore point in their marriage for quite some time.

While flying B-47s, Gregory earned a chance to fly in the US's first high-altitude program, Project Black Knight. This program used modified B-57s for high-altitude reconnaissance. The aircraft consisted of the RB-57-D-0 that performed photographic reconnaissance (13 aircraft), one RB-57-D-1 for radar mapping, and six RB-57-D-2s for electronic intelligence.

The RB-57-D-1 had only one pilot, but various configurations within the other two aircraft had two-man crews (pilot and electronic countermeasures officer) and in-flight refueling capability. These aircraft had a wingspan of 106 feet, twice the wingspan of a B-57. Equipped with the new 10,000-pound-thrust J57 engines with a ceiling of 70,000 feet, they were considered an "overpowered glider."

The RB-57-D-0 had technical problems with its cameras at high altitudes and never met the program requirements; eventually, it was discontinued. Gregory was lucky he was not assigned to that program as originally planned and was instead assigned to the RB-57-D-2 program where he became the project officer for Operation Blue Tail Fly, a detachment officer in charge. He later became the commander of the 4025th Strategic Reconnaissance Squadron at Laughlin AFB, Texas.

Gregory's success as a squadron commander and his performance on deployments, such as Operations Border Town and Sand Shark, led him to be chosen to fly the U-2. The early days of the CIA's U-2 program are discussed as well as the shoot-down of Francis Gary Powers.

Assigned as commander, Detachment G, Edwards AFB (North), California, Gregory worked closely with the CIA and guided the detachment through several projects and deployments. These projects included the Cuban Missile Crisis (he received a personally signed letter from President John F. Kennedy), Vietnam, Thailand, South America, India, and, most interesting of all, taking off and landing the U-2 from an aircraft carrier (Project Whale Tale). The latter included a successful carrier-borne deployment of U-2s to obtain atmospheric readings following nuclear weapons testing in the South Pacific by France. All deployments are further discussed in the book.

After several years with Detachment G, Gregory was offered a chance to become involved with the CIA's Mach 3+ A-12 Archangel program. He declined, having spent so much time away from his family, as the job would mean even more time away. He believed that refusing that assignment likely cost him a star. From Detachment G, Gregory attended the National War College and then took an assignment in the Pentagon on the Air Staff in the Directorate of Reconnaissance and Electronic Warfare, Office of the Deputy Chief of Staff for Research and Development. In 1971, he became the chief of staff for the Air Force Institute of Technology at Wright-Patterson AFB, Ohio.

Gregory retired in 1975 and moved to Austin, Texas, where he had a successful career as the Texas Workers' Compensation Division assistant director. He retired from that position in 1990, and he turned 100 in August 2020.

Spying from the Sky is an interesting read about an Airman's life in the USAF, spent mostly in strategic reconnaissance from World War II to the 1970s. It is also an excellent history of USAF and CIA strategic reconnaissance in the 1950s and 1960s. I highly recommend this book.

Lieutenant Commander Joseph A. Derie, USCG, Retired

Taking Flight: The Nadine Ramsey Story by Raquel Ramsey and Tricia Aurand. University Press of Kansas, 2020, 243 pp.

Taking Flight is the story of a young woman from Wichita, Kansas who became a part of the Women Airforce Service Pilots (WASP). The authors lay the foundation for her story by describing her family and their roots, a family life that played a large role in shaping her into the strong woman she was and how this woman then embraced the growing aviation environment and went on to serve in World War II. Raquel Ramsey, Nadine's sister-in-law, brings a unique perspective on her life and the events that shaped her future.

The book opens with the family's move from El Dorado to life in Wichita as Nadine, a headstrong and independent woman, did not see eye-to-eye with her mother and was unhappy with the move. *Taking Flight* describes the impact that the developing aviation industry in Wichita had on her and how it piqued her initial interest in flying.

A detailed history of other women involved in aviation at the time highlights how they paved the way for women like Nadine to follow in their footsteps. Those changes, and other aviation diversity events during the 1930s, show industry and technology that were evolving, growing, and changing the aviation field leading to trans-Atlantic flight and record-breaking altitude and airspeed records, not just by men but women as well. Nadine Ramsey was in the middle of this, and the authors describe her love of flying and the role that she played with the National Aeronautic Association in developing an aviation ground school at the Wichita Municipal Airport.

The authors give an inspirational overview of the service of women in World War II and how it evolved as the war progressed. As the war broke out, Nadine and her love of flying paved the way for her service in supporting the war effort. The story goes into detail describing the development of the Women's Auxiliary Ferrying Squadron and the Women's Flying Training Detachment (WFTD), services developed so the men could fly in combat and not have to take the time to ferry airplanes to the airfields. It is here that the authors not only describe Nadine's journey but also the lives of the other women who were part of the WFTD—which became the Women Airforce Service Pilots—and the obstacles they faced in society.

The story of the women who served in World War II takes many twists and turns; they began their journey flying planes used for training, and some were qualified to fly twin-engine cargo and transport planes. As the war progressed, the need for fighter aircraft increased as did the women to fly those planes.

The authors describe the training the WASPs experienced to become proficient at flying these aircraft. The women had to spend time in a flight simulator that was a wooden box, situated on bellows so it could rotate and turn. After they completed the flight simulator training, the women advanced to pursuit school where upon graduation they were qualified to fly the P-51 Mustang.

Not everything they faced was positive. In 1944, General Henry "Hap" Arnold cut back the Army Air Forces training programs, and male flight instructors and pilots were suddenly out of work. So these men looked to take jobs ferrying aircraft, and the women faced a change in attitude. It was not only the women involved in flying but also women in other industries who had to deal with this.

This book tells the story of a young woman who seized an opportunity and made the most of it by telling the story of the women who served their country and the sacrifices they made while fighting to gain recognition and honor for their service. Nadine Ramsey was only one of those women, but her story brings them all to the forefront of World War II history, describing the obstacles they faced when they chose to serve their country and the lack of recognition of their service and sacrifice after the war.

Taking Flight is a great addition for anyone interested in women who served their country during World War II, along with wanting to learn about strong women and pass that knowledge onto students or family members.

Steven M. Guiliani