U.S. Marine with Marine Air Control Squadron 1, Marine Air Control Group 38, 3rd Marine Aircraft Wing, assembles communication device during Exercise Summer Fury 20, at Naval Air Weapons Station China Lake, California, July 31, 2020 (U.S. Marine Corps/Juan Anaya)

Fighting as Intended

The Case for Austere Communications

By Scott Pence

It is a law of war: The greater the dependency on a capability, the higher the payoff to an enemy who can lessen its utility, in effect turning our strength into a weakness.

—Colin Gray

Modern command and control (C2) systems depend on connectivity to collect information, issue orders, detect changes in the environment, and exploit successes. While the United States focused on counter-insurgencies in Iraq and Afghanistan, competitors invested in technologies that can neutralize that connectivity. In a conflict, adversaries can distort the reliability of data and degrade U.S. technological dominance. If they succeed in causing degraded operations, adversaries gain a temporary window of superiority that they can develop into a permanent relative advantage.[1] This article offers an overview of threat capabilities juxtaposed with current U.S. joint vulnerability and offers recommendations to reduce risk.

The current suite of digital communications is more advanced and connected than ever before. Investments in network-centric warfare ballooned to the point that all echelons of war, from squad to corps, now possess C2 systems inextricably tied to the space satellite infrastructure and its associated electromagnetic spectrum (EMS) linkages. U.S. C2 systems expedite lethal fire missions from ground, maritime, and air assets;

Colonel Scott Pence, USA, is a Military Faculty Member in the School of Advanced Military Studies at the Command and General Staff College, Fort Leavenworth, Kansas.

enable communications with subordinates to adjust plans and reallocate resources; and integrate intelligence from unlimited sources.

The use of these systems in permissive communications environments obscured their inherent fragility. The 1991 Gulf War highlighted a position of information dominance. When Baghdad fell in 2003 after merely 3 weeks, the commander of Coalition Forces, General Tommy Franks, noted, "The experience was nothing short of religious. I've died and gone to heaven and seen the first bit of network-centric warfare at work!"[2] For a generation, no conventional enemy or violent extremist organization contested U.S. dominance in EMS or threatened the tenuous links to space. Decades of experience in permissive communications environments lulled leaders into thinking perfect situational awareness is a reasonable expectation. It is not. Fog, friction, and uncertainty are intractable features of armed conflict.[3] At the March 2021 Future of Defense Summit, Air Force Chief of Staff General Charles Brown noted, "You can either have information overload or information that is not necessarily clear, or it could be deceptive."[4] An overflow of information is indeed a challenge for today's commanders.

Current C2 systems depend on multiple linkages, and each one is susceptible to enemy disruption. Linkages include the physical network layer (satellites, cables, radio frequencies, routers, switches, and computers), the logical network layer (Web sites and logical programming in cyberspace), and the cyber-persona layer (the digital representation of an individual or entity, email addresses, Internet protocol addresses, and mobile device numbers).[5] Even among the highly digital joint force, the Army depends on space capabilities more than any other Service.[6] Therefore, if an enemy force could deny the reliability and effectiveness of the systems, the disruption would disproportionally affect Army forces.

Known Competitor Capabilities

In 2005, Russian military theorists Makhmut Gareev and Vladimir Slipchenko wrote about the dangers of "non-contact" warfare. They were concerned with the effectiveness of U.S. operations in the Gulf War and later in Serbia: "These wars confirmed [our] hypotheses regarding where we were heading. . . . [The United States] and several NATO [North Atlantic Treaty Organization] countries are moving to a new generation of warfare, the remote, non-contact generation. . . . Those are the types of wars for which Russia must prepare."[7] Gareev and Slipchenko's book, *Future War*, foreshadowed a series of reforms to counter advanced Western technological capabilities. Since then, Russia has invested in cyber warfare, electronic warfare (EW), disinformation campaigns, and the synchronization of each with the others to create lethal strikes.

Chinese doctrine, meanwhile, describes *information warfare* (a combination of electronic warfare and cyberspace operations) as the preeminent form of warfare and explicitly focuses on neutralizing U.S. C2 systems. The 2013 strategy document of the Chinese People's Liberation Army (PLA) stated:

> *The side holding network warfare superiority can adopt network warfare to cause dysfunction in the adversary's command system, loss of control over his operational forces and activities, and incapacitation or failure of weapons and equipment—and thus seize the initiative within military confrontation, and create the conditions for . . . gaining ultimate victory in war.*[8]

A 2015 RAND study reported that the aim of PLA cyber war "is to create information superiority on the traditional battlefield by controlling the flow of information available to the enemy."[9]

Antispace

In 2016, Lieutenant General David Buck, the commander of 14th Air Force, stated, "There isn't a single aspect of our space architecture that isn't at risk."[10] At the time, 14th Air Force was the Service component of U.S. Strategic Command for space operations. Published in 2018, Joint Publication 3-14, *Space Operations*, notes:

> *Our adversaries' progress in space technology not only threatens the space environment and our space assets but could* [also] *potentially deny us an advantage if we lose space superiority. . . . Ground segment assets such as C2 facilities are vulnerable to physical attack and cyberspace attack. The space segment may be vulnerable to attacks from* [antisatellite] *weapons, exoatmospheric nuclear detonations, directed energy weapons, and interference from laser blinding.*[11]

These statements and documents are representative of the consensus among security professionals that current global competitors possess potent antispace capabilities.

A direct ascent antisatellite missile, like the one China tested against its own satellite in 2007, is a possible measure; however, the impact and concomitant debris would have adverse impacts on all countries with space assets.[12] More than a decade after China's antisatellite weapon test, approximately 3,000 pieces of debris remain in space. Satellite operators, therefore, have to conduct collision-avoidance maneuvers any time the orbits transit that debris field. Besides creating space debris, any action that physically destroys a satellite alerts U.S. Strategic Command because satellites perform an important missile detection function, so physical destruction poses serious escalation risks to adversaries. Therefore, kinetic satellite destruction carries high costs for states that depend on the global economy. For rogue states or certain nonstate actors, however, catastrophic global disruption could be the objective.

A much more likely method to deny U.S. network advantages is an electromagnetic attack to jam, monitor, or deceive satellite signals. Both Russia and China optimized their EW enterprise for monitoring, jamming, and deceiving U.S. space-reliant devices.[13] Space capabilities depend on the space segment, link segment, and ground segment. Of the three, the link and ground segments are most vulnerable to EW assets.

Meanwhile, natural events could nullify modern C2 systems without human involvement. Space infrastructure

depends on inherently fragile links in an unforgiving environment, and periodic geomagnetic storms can disrupt a wide range of electronic devices. The Carrington Event of 1859 was a geomagnetic storm that caused telegraph communications around the world to fail. Telegraph operators reported sparks discharging from telegraph machines, shocking the operators, and setting fire to nearby paper. A 2008 National Research Council report noted that a similar event would disable power grids, satellites, and the Global Positioning System (GPS)—and cost over $1 trillion.[14] Whether by human intent or by celestial accident, current mission command capabilities could be denied.[15]

Electronic Warfare

Russia's 2008 incursion into Georgia combined cyber warfare with air and ground maneuver. In the aftermath of the Russo-Georgian conflict, the Russian Federation invested in new EW systems and adapted doctrine, organizations, materiel, and training. The result is a highly capable force integrated into Russian ground forces and equipped with the latest electronic intelligence and jamming systems.[16]

Six years later, the 2014 Russian support to separatists in the Donbas region of Ukraine demonstrated the lethal synchronization of Russian disinformation, cyber warfare, space disruption, EMS dominance, and artillery. The Russians pinpointed Ukrainian positions via the Borisoglebsk-2, a multipurpose EW platform that geolocates, jams, monitors, and even deceives radio and GPS receivers. During the one-sided Battle of Zelenopillya, Russian armed forces electronically geolocated the 79th Ukrainian Airmobile Brigade, confirmed it optically with unmanned aerial systems, and destroyed two Ukrainian mechanized battalions within 30 minutes with a high volume of unguided rockets.[17]

The former commander of U.S. Army Europe, Lieutenant General Benjamin Hodges, noted, "The [Russian] electronic warfare capability—that's something we never had to worry about in Afghanistan and Iraq. . . . You cannot speak on a radio or any device that's not secure because it's going to be jammed or intercepted or worse. It's going to be found, and then it's going to be hit."[18] The 2016 book *The Russian Way of War* catalogs the proliferation of Russian EW organizations, increasing in sophistication from platoon to brigade levels.[19] These EW capabilities have the potential to have cross-domain effects, influencing ground, air, maritime, space, and cyberspace operations.

On the highest end of threats to the EMS is a nuclear high-altitude electromagnetic pulse (HEMP). Each nuclear power has the capability to utilize a HEMP to disrupt all advanced electronic devices within a variable radius. For obvious reasons, HEMPs have not been extensively tested and much of the literature is classified. What is known from Cold War experiments in the 1960s is that any electronic devices exposed become vulnerable to a burst of gamma and X-rays that cause instant damage.[20] When detonated over a city, the collateral damage to the food supply, power generation, and water access would be devastating. If detonated over a remote region, however, a HEMP could deny electronics from facilitating C2 without loss of life. This creates an incredible risk to mission but limited risk to force, as the HEMP destroys electronics but is of little danger to humans. For this reason, the probability of a nuclear-armed power employing a HEMP in a remote operational area is moderate because it could be seen as a reasonable, minimal casualty-producing action that could deescalate a conflict (or neutralize the C2 of Western forces attempting a counteroffensive). The U.S. joint force, dependent on higher end technology for C2, would find itself blinded and deafened in the HEMP area of operations. In response, the U.S. military must consider C2 methods that are either hardened to withstand the effects of a HEMP or are inherently not reliant on the EMS.[21]

Cyber Warfare

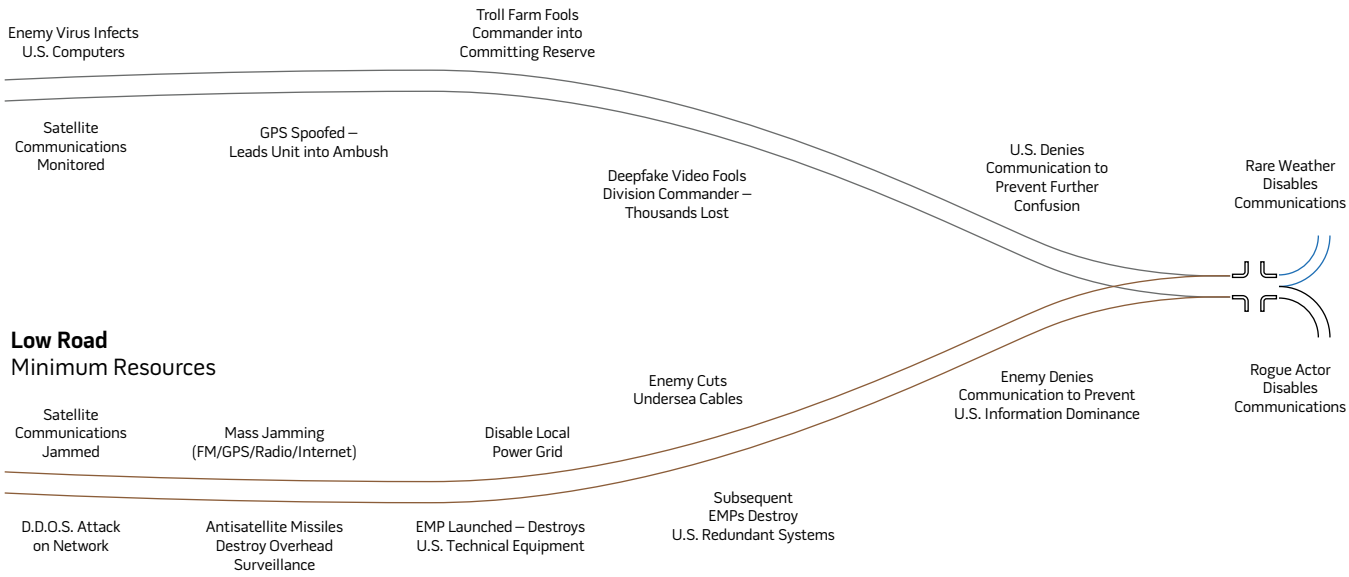
The cyberspace domain is vulnerable due to ease of access, network and software complexity, rogue users, and inherent security design flaws. A single experienced hacker can neutralize an entire network. Effects generated in the cyberspace domain can have significant impacts on the physical domains. These vulnerabilities require continuous and active risk reduction measures.[22]

Russia's 2007 cyber attack on Estonia demonstrated a single-domain attack on a sovereign state's cyberspace. The attack incorporated a distributed denial-of-service attack and debilitated government offices, schools, banks, and hospitals. Since this attack, cyberspace attacks in Georgia, Ukraine, and even the 2016 U.S. Presidential election have been attributed to Russian hackers.[23] These hackers launched a cyber attack on Ukrainian naval headquarters just prior to the 2018 Kerch Strait incident (the seizure of Ukrainian ships on the Sea of Azov). This synchronization of state-sponsored entities and military planning shows the cyber capabilities that the Russian Federation can employ in any military conflict.[24]

China possesses an array of tactical cyberspace capabilities. Recent military reforms integrated China's space, EW, and cyber forces, uniting them under a single command and streamlining their operations for maximum effectiveness. Chinese cyber operations are known for industrial espionage, theft of intellectual property, and breaches into classified U.S. military networks. A 2013 report confirmed that Chinese military hackers were involved in corporate cyber espionage.[25] Thus, Chinese military cyber operations are actively practicing advanced skills in cyberspace through illicit operations that can be militarized in a period of armed conflict.[26]

This cyber warfare capability, practiced by Great Power competitors, can be used in conjunction with antispace and EW capabilities to blind and deafen opponents during armed conflict. To achieve communications denial, the adversary can use all its tools at once or apply them sequentially until they achieve the desired effect. An adversary can apply modest cyber warfare tools like militarized ransomware, distributed denial-of-service attacks, and other tools to

Falcon 9 rocket carrying SpaceX's Starlink L23 payload launches from Cape Canaveral Space Force Station, Florida, April 7, 2021, propelling 60 Internet satellites into space (U.S. Air Force/James Hodgman)



gain access to C2 systems via cyberspace, then progress to unit radios through online routing software. Then an adversary could send viruses via cyberspace to neutralize the connectivity to space assets. Or an adversary could start with a HEMP burst, judge the effects of electronic damage, and use cyberspace and antisatellite tools to complete the communications denial. A sequential method is the most logical because each additional action exposes ostensibly secret adversary capabilities. Alternatively, the adversary could use all capabilities at once to maximize the odds of degrading an opponent's ability to use C2 forces in any coherent manner. The next section postulates how this phenomenon might appear in a future conflict.

Blackout: The Communications-Denied Operational Environment

Competitor states with sophisticated capabilities can create specific zones of communications denial. This militarized blackout condition is a communications-denied operational environment (CDOE).[27] It is an operational blackout that prevents C2 of military forces via space, the EMS, or cyberspace. Within these zones, enemy forces could disrupt, deny, and deceive all communications to the degree that the equipment is unreliable, inoperative, or immediately targetable by enemy destructive effects. When operating in that environment, the U.S. joint force would be vulnerable to tactical disinformation. Adversaries can create a CDOE as an offensive measure in support of their conventional forces or as a defensive tool to stymie an advancing force. Adversary operations will attack C2 systems in the cyberspace domain and the EMS concurrently with attacks on links to space assets. Meanwhile, adversaries could employ their well-honed social and news media disinformation campaigns against joint force headquarters to embarrass and insert doubt into the international narrative. This possibility is particularly salient in adversaries' near-abroad, where their antispace, electronic warfare, and information warfare can synchronize their operations with nearby ground, maritime, and air units.[28]

None of this comes as a surprise to national security professionals; Russian and Chinese investments in niche capabilities are well known and well published in professional journals and national media. Throughout the Department of Defense (DOD), there is widespread appreciation of the current threat to modern C2 systems. U.S. strategic documents highlight the urgency of defending against the advanced capabilities of near-peer competitors.[29]

The figure visualizes the high likelihood of a CDOE and threats to the joint all-domain command and control (JADC2).[30] An adversary can take the high road, which is expensive and resource-heavy, and confuse U.S. forces effectively enough that the United States decides to disable advanced communications to prevent being baited into fratricide and civilian casualties. Alternatively, the adversary can use less expensive existing resources to destroy satellites and advanced equipment by resorting to blunt force (antisatellite missiles, high-altitude electromagnetic pulses, and submarines cutting undersea cables). Meanwhile, the less likely possibility of a rare weather effect or a rogue actor could destroy space infrastructure at any time, leaving relative advantage to the side that is most prepared to operate with austere communication methods.

The Challenges of Fighting Degraded

For commanders and staffs accustomed to accurate situational awareness, the sudden absence of space-enabled imagery, EMS-enabled unmanned aerial systems, and cyber-enabled processes and communication can have a

Sailors conduct preflight checks on E-2C Hawkeye assigned to "Liberty Bells" of Airborne Command and Control Squadron 115 aboard aircraft carrier USS *Theodore Roosevelt*, January 30, 2021, Pacific Ocean (U.S. Navy/Zachary Wheeler)

debilitative effect. Even if the staff had anticipated communications denial and maintained accurate maps and tracking systems, the change from digital fire missions, friendly force tracking, orders dissemination, and intelligence updates to an alternate system would fundamentally uproot the standard operating procedures of the headquarters. Given the best of circumstances and a well-trained organization, the changes require time to adjust, creating a window of opportunity for an adversary to exploit.

Most concerning, information collection and target development are the capabilities most at risk in a CDOE. While some fourth- and fifth-generation aircraft retain capabilities in space-denied conditions, U.S. ground headquarters depend mostly on assets that rely on GPS and satellite communications capabilities. Within a CDOE, manned ground and air reconnaissance forces are critical to observe named areas of interest in support of information collection plans. These forces currently do not exist as formations at the corps and division levels.[31] Meanwhile, information collection processes, analysis, processing, exploitation, and dissemination all require training, standard operating procedures, and organizations that can make sense of the reporting from multiple manned reconnaissance elements. This is a paradigm change from current operations. Manned reconnaissance, on the other hand, depends on human reporting (verbal or written) and relies on the expertise (and cognitive biases) of the reconnaissance scouts. Interpreting information from human sources requires completely different information collection procedures, reporting standards, and intelligence collection matrices that, until trained and rehearsed, will not enable an accurate situational awareness of the operational environment. Fighting with degraded systems, with current organizations that lack manned reconnaissance and security forces at the division or corps level, invites operational surprise.

Recommendations

This article identifies three lines of effort to hedge the joint force against operational surprise:

- continue investments in hardening and countermeasures
- adapt organizations to thrive in CDOEs
- diversify acquisitions with "low-tech" equipment.

Each of these options can be scaled, none is mutually exclusive from another, and prioritization of one or more of them enhances readiness.

Continue Investments in Hardening and Countermeasures. The fiscal year 2020 DOD budget request contained the most substantial investments in research and development request in 70 years, mainly focused on technology.[32] A few of these investments specifically address the vulnerable space, EMS, and cyberspace capabilities of U.S. competitors.[33] DOD requested $1.1 billion to reduce risk to satellite communications jamming, $2.6 billion for cyber operations training, and $5.4 billion to support cybersecurity capabilities.[34] U.S. Army Chief of Staff James McConville noted, "I think what we are trying to do with the Joint All-Domain Command and

Airman uses software to identify interference to specific satellite at Schriever Air Force Base, Colorado, December 16, 2019 (U.S. Air Force/Jonathan Whitely)

Control approach is recognizing that everything we do in the future, we are going to fight jointly." JADC2 will allow the Army to "use all the sensors on the battlefield and get them using technology to get the information to the right shooter," he further explained.[35] These critical investments represent the U.S. Government's commitment to technological dominance.

In the absence of war, advanced C2 systems might appear robust, but warfare exploits every vulnerability. In large-scale combat operations against near-peer adversaries, every technological advance will be met with a countermeasure. Military theorist Edward Luttwak noted that, paradoxically, the best counter to an adversary's strength is not to strengthen the same aspect of one's own forces. He noted, "In the ebb and flow of reciprocal development, the same device could be highly effective when originally introduced, then totally useless, and finally positively dangerous, and all within a matter of months."[36] During World War II, the British fitted rearward-looking radars to their bombers to warn that fighters were nearby. These saved lives initially, but then the Germans developed a system that honed onto them and pinpointed the bombers at night. This made the rearward-looking radars worse than useless; they were a direct danger if used. Luttwak went on to explain, "As soon as a significant innovation appears on the scene, efforts will be made to circumvent it—hence the virtue of . . . suboptimal but more resilient solutions."[37] Investments in new and better technology are necessary but cannot guarantee a relative advantage.

Furthermore, technological investments are costly to create and to maintain. As anyone who has worked in the "blocks" section of a child daycare knows, it is much easier to destroy than to create or maintain. Systems depending on redundancy for risk mitigation can be parried by repeated destruction. Therefore, any robust solution must be able to withstand simple destruction by known adversary capabilities.

Adapt Organizations to Thrive in CDOEs. In addition to continued investments in advanced technology, the U.S. military could adapt specific units to accomplish missions with systems that do not depend on space, the EMS, and cyberspace. Given known capabilities, operations within the near-abroad of any current competitor present a significant challenge with existing forces—their antispace, EW, and cyberspace capabilities can neutralize U.S. C2 systems indefinitely. Strategist Everett Dolman wrote, "It is the height of folly for a commander to rely on a capacity that may or may not be available when needed."[38] Therefore, remove the systems from specialized units and man, train, and equip them for mission accomplishment in CDOEs.

By adapting a portion of the joint force to operate without dependence on known C2 vulnerabilities, DOD

could hedge against a likely operational environment—one in which modern communications are denied in whole or in part. And these forces, optimized for operations within an enemy's antiaccess/area-denial (A2/AD) area, could accomplish missions that set conditions for joint all domain operations.[39]

To resolve current shortfalls, organizational adaptations should reduce features with known vulnerabilities (space, EMS, and cyber-reliant C2 systems) and add features that would enhance operations in a CDOE. Changes should retain (or improve) lethality and maneuverability while reducing the electromagnetic signature of the organization. An increase in headquarters personnel for battle tracking and courier operations, for example, could be paired with the reduction in computer network personnel. With a focus on enhancing capability and reducing exposure, leaders could optimize a unit capable of sustained mission accomplishment within a CDOE.

This is not as simple as just taking the vulnerable C2 systems out of formations; the manning, training, and equipment all require integration. The Army's multidomain concept requires "formations that have systems, leaders, and Soldiers that are durable, can operate in a highly contested operational environment, cannot easily be isolated from the rest of the joint force or from partners, and can conduct independent maneuver and employ cross-domain fires."[40] A specialized force, without vulnerable dependencies on satellite, cyber, and the EMS, would begin preparations for the mission using austere tools optimized for mission accomplishment within CDOEs. Maneuvering with minimal EMS emissions, they would frustrate the enemy's preferred methods of detection and approach the threat systems that created the CDOE. The specialized force would use volumes of firepower and maneuver to dis-integrate the enemy's A2/AD assets and deny the ability to sustain the CDOE. Once the operational blackout lifts, follow-on forces with the latest and most efficient suites of C2 systems would arrive to consolidate gains and exploit success with the full convergence of joint force capabilities.[41] In this way, less connected forces facilitate the entry of the most connected forces to positions of advantage.

Diversify Acquisitions with "Low-Tech" Equipment. Eliminating the reliance on space, the EMS, and cyber does not mean the United States needs to revert to telegraphs and smoke signals for communication. Diverse equipment increases the dilemmas a potential adversary must address. While it is convenient for acquisitions and budget professionals to populate units with like equipment, a homogenous force also enables the threat to focus on a predictable set of targets.

Considerations for material decisions include legacy equipment, complementary equipment, alternative technology, and dual-use acquisition mandates. Legacy equipment includes materiel solutions that no longer reside in U.S. military inventories. Units need communication wire, fiber optic cable, and tactical phones to communicate in assembly areas without transmitting over the EMS. Manual signal operating instruction systems enable operational, secure message exchanges. Light mobility vehicles, rugged 4x4s, and militarized motorcycles can allow effective courier operations for mission orders and information management.

Complementary equipment includes advanced camouflage and decoy systems. These capabilities are expensive to field to the entire force but would add protection in a CDOE. Modern camouflage has varied thermal panels and location-specific color patterns that offer advanced protection from observation by thermal and optical sights. Electronic decoys and EMS-emitting devices that give false targets for adversaries to target enhance a unit's protection plan. Modern EMS-emitting decoys could broadcast headquarters radio and satellite communications signals from a location separate from actual forces, make one headquarters look like many headquarters, or purposely broadcast deception narratives.

Alternative technologies could exploit modern advancements while avoiding an overreliance on space-, EMS-, and cyberspace-based systems. Integrated tactical networks, which create pseudo-cellular networks with military devices, can provide encrypted communications without betraying locational data.[42] A CDOE-optimized force could use a mixture of austere and modern advanced systems to accomplish missions and provide heterogeneous capabilities to the joint force.

When it comes to partner-nation interoperability, low-tech can result in big gains. The U.S. joint force, with its highly specialized communications platforms, struggles to communicate with international partners. Both the European and Indo-Pacific combatant commands list interoperability as a critical challenge to overcome with partnered units. In Europe, NATO standards allow communications across cyber channels and along the EMS. However, few nations have advanced compatible systems that can communicate with those of the United States. The scale of challenges increases every time the United States issues more advanced technology to its forces. By diversifying C2 technology with less advanced systems, the capacity for interoperability increases.

Positive developments exist in every Service, as leaders reconsider the tactics, techniques, and procedures that worked in a period of information dominance but are uncertain in large-scale combat against a near-peer. The U.S. Air Force Pacific's plan for agile combat employment innovations can provide multiple dilemmas to adversaries.[43] The U.S. Naval Academy in 2016 reinstituted celestial navigation into its navigation curriculum.[44] And the U.S. Space Force deployed ground-based counter-satellite communications stations in 2020.[45]

Conclusion

Because operations in CDOEs are so likely, the joint force requires alternative means to gain access, accomplish missions, and enable all-domain operations within them. As long as competitors possess capabilities that can significantly affect joint operations, the joint force has a responsibility to develop solutions to ensure the accomplishment of missions. And those innovative solutions need not always be new and better technology.

Airman with 379th Expeditionary Operations Support Squadron Silent Sentry adjusts antenna to maximize signal strength from orbiting satellite, May 27, 2015, at Al Udeid Air Base, Qatar (U.S. Air Force/Alexandre Montes)

This article contributes to the body of work on avoiding defeat in the first battle of the next war. The first battle of Savo Island, August 1942, was a tragic failure. The U.S. Navy lost multiple ships and over 1,000 Sailors. Historian Robert Frank noted:

The Navy was still obsessed with a strong feeling of technical and mental superiority over the enemy. In spite of ample evidence of enemy capabilities, most of our officers and men despised the Japanese and felt themselves sure victors in all encounters under any circumstances. The net result of all this was a fatal lethargy of mind which induced a confidence without readiness.[46]

Decades of technological superiority biased our senior leaders with false confidence in modern C2 systems. To avoid accusations of a "fatal lethargy of mind" on the next generation, military professionals should recognize their hubristic biases toward technological solutions. With forces capable of accomplishing missions as intended, not degraded, in communications-denied environments, the U.S. military gains a strength, not a liability. **JFQ**

Notes

[1] Field Manual (FM) 3-0, *Operations* (Washington, DC: Headquarters Department of the Army, October 2017), 1–4.

[2] Office of Force Transformation, *The Implementation of Network-Centric Warfare* (Washington, DC: Department of Defense, 2005), 18.

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

[4] Matthew Cox and Oriana Pawlyk, "These 4-Stars Want to Help Commanders Avoid Information Overload in the Next War," *Military.com*, March 30, 2021, available at <https://www.military.com/daily-news/2021/03/30/these-4-stars-want-help-commanders-avoid-information-overload-next-war.html>.

[5] FM 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: Headquarters Department of the Army, 2017), 1-13–1-14.

[6] FM 3-14, *Army Space Operations* (Washington, DC: Headquarters Department of the Army, 2019), 1-1.

[7] Makhmut Gareev and Vladimir Slipchenko, *Future War* (Fort Leavenworth, KS: Foreign Military Studies Office, February 2007), 13.

[8] Shou Xiaosong, ed., *The Science of Military Strategy*, 3rd ed. (Beijing: Military Science Press, 2013), 189.

[9] Eric Heginbotham et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017* (Santa Monica, CA: RAND, 2015), 274.

[10] Jonathan Broder, "Why the Next Pearl Harbor Could Happen in Space," *Newsweek*, May 4, 2016.

[11] Joint Publication 3-14, *Space Operations* (Washington, DC: The Joint Staff, April 10, 2018), I-7.

[12] Shirley Kan, *China's Anti-Satellite*

Weapon Test, RS22652 (Washington, DC: Congressional Research Service, April 23, 2007); FM 3-14, 1-12.

[13] Lester W. Grau and Charles K. Bartles, *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces* (Fort Leavenworth, KS: Foreign Military Studies Office, 2016); Paul McLeary, "Red Electrons: Army Rapid Capabilities Office Fights Russian GPS Jamming, Cyber, EW," *Breaking Defense*, November 22, 2018, 1–10.

[14] National Research Council, *Severe Space Weather Events—Understanding Societal and Economic Impacts: A Workshop Report* (Washington, DC: National Academies Press, 2008), 104.

[15] Christopher Klein, "A Perfect Solar Superstorm: The 1859 Carrington Event," *History*, March 14, 2012.

[16] Grau and Bartles, *The Russian Way of War*, 289.

[17] Samuel Cranny-Evans, Mark Cazalet, and Christopher F. Foss, "The Czar of Battle: Russian Artillery Use in Ukraine Portends Advances," *Jane's International Defence Review*, April 24, 2018, available at <https://customer.janes.com/Janes/Display/FG_901376-IDR>.

[18] Mike Eckel, "Ex-U.S. Army Commander Warns of Russian Capabilities in Ukraine," Radio Free Europe/Radio Liberty, January 24, 2018, available at <https://www.rferl.org/a/ukraine-drones-artillery-ukrainian-forces/28994516.html>.

[19] Grau and Bartles, *The Russian Way of War*.

[20] Conrad L. Longmire, "On the Electromagnetic Pulse Produced by Nuclear Explosions," *IEEE Transactions on Electromagnetic Compatibility* 26, no. 1 (January 1978), 3–13.

[21] Edward Savage, James Gilbert, and William Radasky, *The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid* (Goleta, CA: Metatech Corporation, January 2010), 11–12, 168.

[22] FM 3-12, 1–67.

[23] Roger N. McDermott, Bertil Nygren, and Carolina Vendil Pallin, eds., *The Russian Armed Forces in Transition: Economic, Geopolitical, and Institutional Uncertainties* (Abingdon-on-Thames, UK: Routledge, 2012); Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, DC: Department of Justice, March 2019), 36–40.

[24] Stephen Blank, "Cyber War and Information War à La Russe," in *Understanding Cyber Conflict: 14 Analogies*, ed. George Perkovich and Ariel E. Levite (Washington, DC: Georgetown University Press, 2017), 85–89; Mueller, *Russian Interference in the 2016 Presidential Election*, 36–41; Patrick Tucker, "Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Says," *Defense One*, December 7, 2018.

[25] *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant Corporation, February 13, 2013), 20, available at <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.

[26] Heginbotham, *The U.S.-China Military Scorecard*, 271.

[27] The term *communications-denied operational environment* more broadly integrates the convergence of antispace, electronic warfare, cyber warfare, and information warfare effects than does the closest doctrinal term, *disrupted, degraded, and denied space operational environment*, which primarily focuses on the space domain.

[28] FM 3-0, I-4.

[29] *National Security Strategy of the United States of America* (Washington, DC: The White House, 2017), 27.

[30] John R. Hoehn, *Joint All-Domain Command and Control: Background and Issues for Congress*, R46725 (Washington, DC: Congressional Research Service, March 18, 2021), available at <https://crsreports.congress.gov/product/pdf/R/R46725/2>.

[31] Nathan Jennings, "Fighting Forward: Modernizing U.S. Army Reconnaissance and Security for Great Power Conflict," *Military Review* 99, no. 6 (December 2019), 100–108.

[32] Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Defense Budget Overview: Fiscal Year 2020 Budget Request* (Washington, DC: Department of Defense, March 2019), 1–9.

[33] Ibid., 4–13.

[34] *National Defense Authorization Act for Fiscal Year 2020*, Pub. L. 116–92, 116th Cong., 1st sess., December 20, 2019, available at <https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf>.

[35] Cox and Pawlyk, "These 4-Stars Want to Help Commanders Avoid Information Overload in the Next War."

[36] Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, MA: Belknap Press, 2002), 29.

[37] Ibid., 31.

[38] Everett Carl Dolman, "New Frontiers, Old Realities," *Strategic Studies Quarterly* 6, no. 1 (Spring 2012), 88.

[39] TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018).

[40] Ibid., xii.

[41] Ibid.

[42] Matthew S. Blumberg, "The Integrated Tactical Network: Pivoting Back to Communications Superiority," *Military Review* 100, no. 3 (2020), 104–115.

[43] Amy McCullough, "Ace in the Hole," *Air Force Magazine*, March 30, 2017, available at <https://www.airforcemag.com/article/ace-in-the-hole/>.

[44] Devin Arneson, "Charting a New Course: Celestial Navigation Returns to USNA," *CHIPS*, October 16, 2015, available at <https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=7000>.

[45] Sandra Erwin, "U.S. Space Force Gets Upgraded Satellite Communications Jammers for 'Offensive' Operations," *Space News*, February 4, 2020, available at <https://spacenews.com/u-s-space-force-gets-upgraded-satellite-communications-jammers-for-offensive-operations/>.

[46] Richard B. Frank, *Guadalcanal: The Definitive Account of the Landmark Battle* (New York: Penguin Group, 1990), 123.