Four Army CH-47F Chinook helicopters from 1st Battalion, 214th Aviation Regiment (General Support Aviation Battalion), 12th Combat Aviation Brigade, prepare to land during exercise Falcon Autumn 22 at Vredepeel, Netherlands, November 4, 2022 (U.S. Army/Thomas Mort)

A Mission Assurance Assessment of Threats to Missions and Force Protection Planning

By Michael J. Borders, Jr., and Miller Carbaugh

After the Cold War, the United States enjoyed such an uncontested or dominant superiority in every domain that the Department of Defense (DOD) could deploy forces when it wanted, assemble them where it wanted, and operate them as it wanted. Perhaps because of this history, combined with the objectives in the 2018 National Defense Strategy (NDS), DOD components have focused on the development of new offensive and lethal capabilities and concepts with the unstated assumption that, once developed, these capabilities would be available. The following scenario describes how these assumptions can adversely affect DOD force projection capabilities.

A crisis occurs, a combatant commander is assigned to respond by using a specific operations plan or developing

Colonel Michael J. Borders, Jr., is the Commander of Detachment 3, Air Force Installation and Mission Support Center, Hurlbut Field, Florida. Miller Carbaugh is a People Operations Generalist at the Heritage Foundation.

Soldier assigned to Force Protection Platoon, 3rd Battalion, 66th Armored Regiment, 1st Armored Brigade Combat Team, 1st Infantry Division, maintains perimeter security from top of Humvee during gate runner exercise conducted at Camp Herkus, Lithuania, April 13, 2022 (U.S. Army National Guard/Agustín Montañez)

a contingency plan, and forces begin to flow. However, what if the forces that enable either of these plans are delayed or reduced, or they do not show up at all? Claiming that this could never happen or that we would "figure it out" is not sufficient. There is a serious need for a better response. If, at all levels of command, these forces are delayed, degraded, or completely unable to function as needed, then the joint force commander's decision space is reduced, adversely affecting the decisionmaking process and ultimately risking mission failure.

The Current Security Environment

The unclassified 2018 summary of the NDS states that "the homeland is no longer a sanctuary" and notes that the United States faces, among other challenges, a "reemergence of long-term strategic competition." Strategic competition in this environment "requires the seamless integration of multiple elements of national power—diplomacy, information, economics, finance, intelligence, law enforcement, and military."[1]

The security environment is described here as one in which terrorism remains a persistent condition, transnational criminal organizations and other malicious nonstate actors have increasingly sophisticated capabilities, and revisionist powers and rogue regimes will use ambiguous or denied proxy operations to achieve their ends short of open warfare.[2] Adversaries have enjoyed the opportunity to identify and categorize critical capabilities and associated vulnerabilities of the joint force; their resulting strategies could create confusion, disrupt or delay force projection, and divert military resources in the transition to war.

Great Powers and rogue regimes have been able to conduct a campaign of operational preparation of the environment (OPE) nearly autonomously both inside and outside the continental United States (OCONUS). Current U.S. protection efforts do not align with the threats outlined in the NDS and endanger DOD's ability to flow forces from the homeland to OCONUS combatant commanders, increasing the risks associated with projecting military power. Adversaries are improving their existing capabilities and seeking new, asymmetric means to delay, disrupt, and cripple our force projection, warfighting, and sustainment capabilities by targeting military and civilian infrastructures—within the homeland and abroad—that our military forces depend on.

Campaigns Against Critical Infrastructure

The building blocks that DOD needs to conduct successful military campaigns in the Great Power era are predominantly located on its installations and bases across the homeland. These building blocks are reliant on critical infrastructure located both inside and outside the boundaries of DOD authorities and control. Key questions to consider are:

- How do commanders ensure they can project forces forward when projection relies on critical infrastructure outside their authority and is exposed/targeted for nontraditional attacks?
- What are the nicks and cuts our adversaries can inflict on this critical infrastructure that commanders must account for, and how can they work to mitigate these?

Regarding these questions, specifically concerning China and Russia, the Office of the Director of National Intelligence warns:

> *China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States. . . .*
>
> *Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.*[3]

Recent Targeting Activities by Adversaries

Adversaries are conducting OPE and actively targeting U.S. critical infrastructure through hybrid and blended operations that take advantage of legal restrictions and friction points between U.S. departments and agencies. Their overarching goal is to hold our centers of gravity at risk and impact force projection; they are capable also of sowing discontent during steady-state activities and therefore of ultimately destabilizing and delegitimizing our government. Their near-term goals are simply to identify and categorize attack vectors in the event of a larger conflict. Examples over the past few years include:

- Software engineer Xudong "William" Yao was wanted for theft of proprietary information, including nine copies of control system source code and systems specifications from a Chicago locomotive manufacturer in 2019. He remains at large and is suspected of having returned to China.[4]
- More than two dozen U.S. universities were targeted by Chinese hackers in 2019 as part of an effort to steal military maritime technology research.[5]
- In 2020, there was an attempt to disrupt the power grid by drone, when a DJI Mavic 2 approached a Pennsylvania power substation with intent to "disrupt operations by creating a short circuit."[6] This was the first known instance of a modified, uncrewed aircraft system being used to specifically target U.S. energy infrastructure.[7]
- Russian state-sponsored advanced persistent threat actors targeted state, local, tribal, and territorial governments, and aviation networks in 2020, successfully compromising networks and exfiltrating data from multiple victims.[8]
- In 2019, the U.S. Cybersecurity and Infrastructure Security Agency warned of the possible cyberespionage threat that Chinese-made drones could pose to U.S. businesses and other organizations that use them.[9] The notice added that those most at risk were using the aircraft for tasks related to national security or critical infrastructure.[10]
- Zhao Qianli, student tourist in Florida, accessed and photographed U.S. Naval Air Station Key West, Joint Interagency Task Force South; he was detained through close base police–local police cooperation and was sentenced to prison, in 2019, for illegal photography of the air station.[11]
- A National Security Agency senior official warned about rising Chinese hacking against United States in 2018, noting that the hackers were targeting critical infrastructure in possible attempts to lay the groundwork for future disruptive attacks.[12]
- According to a 2019 report by Vietnam Veterans of America, Russian information operations are increasingly targeting troops, veterans, and their families, connecting with prominent members to shape Federal policy with the goals of perpetrating financial fraud, spreading anti-American propaganda, manipulating online public spaces, and sowing discord by exploiting and inflaming national divisions.[13]
- Russian aluminum giant Rusal, previously sanctioned by the United States, purchased a 40 percent stake in an Ashland, Kentucky, plant in 2019. The Kremlin-linked firm invested millions of dollars, raising both economic and national security concerns.[14]
- In 2018, intelligence analysts warned that Russian hackers probing the U.S. power grid were achieving many goals through persistent probing; the full extent of their access is largely unknown.[15]
- A Justice Department official warned in 2020 that homegrown violent extremists could potentially weaponize the COVID-19 virus and use it against the populace.[16]

As these examples demonstrate, gray zone warfare is being conducted both inside and outside the wire in cyberspace. Adversaries will operate in any domain where they perceive they can gain an advantage. Their ongoing OPE requires them to be patient and imaginative and to stay in it for the long haul.

Nonlinear and Nontraditional Way Forward

To ensure force projection from the homeland, DOD must focus sufficient attention on protecting competitor and adversary activities in the steady state short of war (gray zone threats) to protest adversary activities in the transition to war. This distinction is perhaps useful for discussion purposes, but the transition between the two conditions, in

Marine Corps AV-8B Harrier attached to 22nd Marine Expeditionary Unit flies past Navy Aviation Boatswain's Mate (Handler) 1st Class Tu N. Chau during flight operations aboard USS *Kearsarge* in Baltic Sea, August 24, 2022 (U.S. Navy/Taylor Parker)

reality, might not be clear until after it has occurred. Implicit in this limited examination is an assumption that war plan development and review fully consider the spectrum of adversary capabilities.

Through a rigorous assessment of the range of competitors and potential adversaries, their anticipated operational concepts, and their technological tools, DOD must anticipate military problems of future conflict and develop its own operational concepts, both offensive and defensive, to ensure that the joint force can react, deploy, survive, operate, maneuver, and regenerate. Essentially, if the United States wants to deploy forces from a contested homeland in the future, it must think differently about how, where, and with whom it protects those forces in the homeland, starting now. The following represent discussion points and recommended ways to move the conversation forward.

Analyze Competitors, Adversaries, and Capabilities. The need to defend against terrorism is not going away. A new normal exists, with an ever-present, evolving global terrorist threat. However, DOD has a wider range of competitors, potential adversaries, and natural and manmade hazards to consider. Terrorists, insurgents, and those who present the greatest risk to the Nation must not be the only priority; the COVID-19 pandemic serves as an excellent real-life example of a biological hazard's disruption of military operations. A logical first step in planning is to analyze what capabilities DOD may have to counter, now and in the future. This will, of course, have to be a continuous process of identification, evaluation, and red-teaming or wargaming that fleshes out actual threat and hazard capabilities, potential consequences, and useful countermeasures to drive adaptation at the speed of relevance. This wargaming will have to assume an effective coordinated first punch—with an indeterminable amount of ambiguity following.

The challenge during steady-state operations is that even potential adversaries who pose the greatest risk can minimize their exposure by pretending to be what they are not, through denied or proxy operations and the exploitation of commercially available technology. Therefore, assessing capabilities and creative employment potential is likely a more useful start than trying to identify specific potential adversary or competitor users in advance.

Superior capabilities of the Great Powers and rogue regimes are most dangerous; they require additional analysis of where, when, how, and why they might be used. Such actors may use them in gray zone activities, during the transition to war, and/or during conflict. Although these capabilities are probably already

captured through an existing intelligence requirement, their potential impact on future force protection needs must be the focus of analysis. This analysis must adjust as necessary.

Analyze DOD, Interagency, Allied, and International Partner Capabilities. Addressing existing challenges requires an assessment of available tools and resources for use in the present. Numerous programs and processes exist to protect DOD personnel, resources, assets, systems, facilities, and information, though they are not currently optimized for the changing security environment. These programs and processes include but are not limited to antiterrorism; law enforcement; physical, information, industrial, personnel, operations, and cyber security; and counterintelligence. Additionally, given the potential of biological threats, force health protection must be part of this analysis. For the near term, a sufficient assessment of the existing capabilities and capacities of these programs and processes will inform an analysis of potential gaps to follow.

Any such assessment would be incomplete without considering partnerships with interagency and international partners. Numerous Federal agencies, state and local authorities, allies, and other international partners, each with its own source and limit of authority, have capabilities relevant to protecting the joint force. A complete characterization of all these entities is unnecessary at the macro level, though protection planning at each successive level of command must adequately engage the relevant partner organizations in the area. Also, an important consideration in this process is the impact of the security environment on the existing mission and ability of each of these entities to protect relevant populations and infrastructure. Because they all must cope with finite resources and expanding challenges, identifying efficient and effective means of mutual support will be an ongoing effort.

Identify and Prioritize Gaps and Excesses. With the NDS defining the strategic endstate, the analysis of current and projected adversary capabilities and DOD and partner capabilities defines the starting point. Capability and/or capacity mismatches indicate potential gaps and excesses to prioritize and address. Because any initial analysis will become obsolete quickly in a rapidly changing environment, an iterative process will be necessary to identify new conditions, their influence on existing capabilities, capacities, and excesses, and any changes to gap-solution priorities. Such an effort will require the participation of and coordination among U.S. departments and agencies.

Develop and Implement Solutions. The existing DOD process to identify potential solutions in doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy is a valid approach. To anticipate, analyze, decide, and develop countermeasures at the speed of relevance will likely require new processes that produce some results sooner, which are preferable to comprehensive results that come too late. Speed of action has inherent risk, but the production of faster results is worth this risk.

To ensure DOD employs effective deterrent effects against near-peer aggression, it should develop a special operations forces hybrid warfare capacity focusing on U.S. critical infrastructure. It should determine vulnerabilities and recommend ways to harden U.S. critical infrastructure against exploitable vectors, and build an offensive capability to exploit similar vulnerabilities in revisionist nations. To confidently project power in the gray zone, the U.S. Government must secure our domestic power projection platforms to deny reciprocal strategies from our strategic competitors.

Focus on the Installation Level. Commanders must now distill the previous four discussion points into an applicable approach at the local level. There must be a recognition that OPE campaigns are ongoing and focused on the U.S. critical infrastructure that enables force projection. Recognizing the analysis and thorough mission decomposition of the specific forces projected forward is key. Successful force projection will likely rely on U.S. critical infrastructure both on and off DOD installations. This process will require a ruthless determination of what is important and how to defend it. The shift in adversary tactics will require installation commanders to develop and implement a more synergized and integrated approach, with intelligence, cyberspace, security, local law enforcement, and other efforts all playing their part to protect the reliant critical infrastructure wherever necessary.

Conclusion

The NDS identifies persistent and rising threats to the homeland, but current legal considerations, especially restrictions, are a challenge. Adversaries continue to conduct OPE in the near term and take advantage of friction points within the U.S. Government. To protect the homeland, new methods, authorities, and partnerships are required. However, mission owners must start with a prioritization of what enables their mission that extends beyond the wire so that they may be better prepared to answer if forces are delayed, reduced, or unable to show up when a crisis occurs.

DOD leaders will need to rethink how they will execute missions—not only the initial deployments or dispersals but also all activities leading up to the execution order. DOD needs to incorporate real resilience, as well as physical and cyberspace protection, in all its capabilities—supply chain, mission operations, personnel management, and command and control. As expressed in the discussion and recommendations, DOD needs the support of the whole of government, and in many instances the whole of society, to enable it to execute its missions with minimal delays and disruptions. To fail to provide such support will be playing into our adversaries' hands, and history will repeat itself—perhaps with much more devastating consequences. JFQ

Notes

[1] *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), available at <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

[2] Ibid.

[3] *Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2019), available at <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>.

[4] "Newly Unsealed Federal Indictment Charges Software Engineer with Taking Stolen Trade Secrets to China," Department of Justice, July 11, 2019, available at <https://www.justice.gov/opa/pr/newly-unsealed-federal-indictment-charges-software-engineer-taking-stolen-trade-secrets-china>.

[5] Dustin Volz, "Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets," *Wall Street Journal*, March 5, 2019.

[6] Brian Barrett, "A Drone Tried to Disrupt the Power Grid. It Won't Be the Last," *Wired*, November 5, 2021, available at <https://www.wired.com/story/drone-attack-power-substation-threat/>.

[7] Ibid.

[8] *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure* (Washington, DC: Cybersecurity and Infrastructure Security Agency [CISA], January 11, 2022), available at <https://www.cisa.gov/uscert/ncas/alerts/aa22-011a>; "Unmanned Aircraft Systems (UAS)—Critical Infrastructure," CISA, February 15, 2017, available at <https://www.cisa.gov/unmanned-aircraft-systems>.

[9] "U.S. Warns of Threat from Chinese Drone Companies," BBC News, May 21, 2019, available at <https://www.bbc.com/news/technology-48352271>.

[10] "Unmanned Aircraft Systems (UAS)."

[11] "Chinese National Sentenced to Prison for Illegal Photography of U.S. Naval Installation in Key West, Florida," Department of Justice, 2019, available at <https://www.justice.gov/usao-sdfl/pr/chinese-national-sentenced-prison-illegal-photography-us-naval-installation-key-west>.

[12] Jim Finkle and Christopher Bing, "China's Hacking Against U.S. on the Rise: U.S. Intelligence Official," Reuters, December 11, 2018, available at <https://www.reuters.com/article/us-usa-cyber-china/chinas-hacking-against-u-s-on-the-rise-u-s-intelligence-official-idUSKBN1OA1TB>.

[13] Kristofer Goldsmith, *An Investigation Into Foreign Entities Who Are Targeting Servicemembers and Veterans Online* (Silver Spring, MD: Vietnam Veterans of America, 2019, available at <https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf>.

[14] Simon Shuster and Vera Bergengruen, "A Kremlin-Linked Firm Invested Millions in Kentucky. Were They After More Than Money?" *Time*, August 13, 2019, available at <https://time.com/5651345/rusal-investment-braidy-kentucky/>.

[15] Lily Hay Newman, "Russian Hackers Haven't Stopped Probing the U.S. Power Grid," *Wired*, November 28, 2018.

[16] Betsy Woodruff Swan, "How the Coronavirus Is Reshaping Terrorists' Attack Plans," *Politico*, March 27, 2020, available at <https://www.politico.com/news/2020/03/27/coronavirus-terrorism-justice-department-150870>.