Interim Armored Vehicle "Stryker" and AH-64 Apache helicopters with Battle Group Poland move to secure area during lethality demonstration at Bemowo Piskie Training Area, Poland, June 15, 2018, as part of Saber Strike 18 (U.S. Army/Hubert D. Delany)

Strengthening Mission Assurance Against Emerging Threats

Critical Gaps and Opportunities for Progress

By Paul N. Stockton with John P. Paczkowski

U.S. combatant commanders (CCDRs) face an intensifying and deeply asymmetric challenge to carrying out their operational plans (OPLANs). To help execute these plans, Department of Defense (DOD) facilities and functions require electric power and other infrastructure support, typically provided by U.S. civilian-owned utilities (or host-nation assets for installations abroad). Disrupting or destroying that infrastructure offers adversaries an indirect but potentially devastating means to degrade the deployment, operation, and—ultimately—the lethality of U.S. combat forces.

Since publication of the DOD *Mission Assurance Strategy* in 2012, the Department has taken far-reaching measures to strengthen mission assurance (MA).[1] In particular, DOD has expanded its traditional emphasis on defense critical infrastructure protection and is adopting a more holistic and integrated approach

Dr. Paul N. Stockton is Managing Director of Sonecon, LLC. From 2009 to 2013, Dr. Stockton served as Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs. Colonel John P. Paczkowski, USMCR (Ret.), is Senior Managing Director at Witt O'Brien's.

to support OPLAN execution by regional and functional combatant commands (CCMDs). DOD is also improving the resilience of critical nodes for defense functions and advancing new partnership initiatives with private-sector infrastructure owners and operators.

However, potential adversaries are refining increasingly sophisticated cyber weapons to disrupt and destroy industrial control systems and other key enablers of the electric grid, water systems, ports, and other support functions. Private-sector infrastructure owners and operators are also increasingly concerned that adversaries will combine cyber attacks with information warfare and kinetic strikes against key system nodes. Moreover, for installations abroad that rely on host nation–supplied energy, or on infrastructure owned and operated by Russian and Chinese companies, a simple flip of the switch could jeopardize mission execution.

DOD should counter these intensifying threats by intensifying the MA focus on supporting OPLAN execution. Exercises that assess how disruptions in U.S. infrastructure might affect the flow of forces, logistical support, and other components of such plans can help identify opportunities to strengthen MA and help DOD move beyond outdated debates over investing in "tooth versus tail." The Department should also bring cybersecurity into the heart of mission assurance and intensify the DOD focus on managing the risks posed by wide-area, long-duration power outages. However, MA initiatives should also account for the danger that adversaries will strike energy systems with both cyber and physical attacks. Moreover, adversaries could attack multiple sectors simultaneously and intensify the cascading failures between them.

Mission Assurance: Basic Goals and Ongoing Progress

The 2018 National Defense Strategy emphasizes that "the *homeland is no longer a sanctuary*." It also notes that "during conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated."[2] Especially significant, adversaries may strike the infrastructure that DOD relies on to carry out its mission essential functions (MEFs) and undermine the lethality of the joint force.[3]

Mission Assurance Strategy provides the foundation to meet these challenges. The strategy highlights how adversaries can seek "asymmetric means to cripple our force projection warfighting, and sustainment capabilities by targeting critical defense and supporting civilian capabilities and assets." The strategy also offers overarching guidance to strengthen mission assurance—that is, by building "a comprehensive and integrative framework to assess and address risks" to MEFs and using that framework to help "prioritize investments to ensure MEF performance in a constrained fiscal environment."[4]

The issuance of DOD Directive 3020.40, *Mission Assurance*, in November 2016 marked a major step forward in implementing that vision. The directive remedies a key gap in the 2012 strategy by integrating cybersecurity issues into mission assurance. The directive also strengthens DOD-wide governance and coordination mechanisms for mission assurance. Especially valuable, the document directs DOD components to prioritize MA efforts to help fulfill critical DOD strategic missions, including CCDR execution of OPLANs.[5]

DOD components are also accelerating their efforts to strengthen mission assurance. The military departments, Joint Staff, CCMDs, and other components are refining their own plans and risk mitigation strategies for MA. Moreover, they are increasing collaboration across the Department to develop holistic approaches to support CCMD OPLAN execution. However, threats to mission assurance are becoming more severe and increasingly diverse. Understanding these threats and the asymmetric strategies that leverage them is essential for assessing potential gaps in MA plans and capabilities and for developing initiatives to address these shortfalls.

Emerging Threats to Mission Assurance

The most rapidly intensifying challenges to mission assurance stem from the risk of cyber attacks on the electric power grid, transportation systems, and other civilian-owned infrastructure that defense operations depend on. This section also examines the risk that adversaries will combine cyber attacks with targeted kinetic strikes and information operations to cripple the restoration of electric power and other defense-critical services.

Cyber Attacks on the Grid and Other Supporting Infrastructure. Former U.S. Director of National Intelligence Dan Coats warned that "today, the digital infrastructure that serves this country is literally under attack."[6] Russia and other nations are conducting sustained, increasingly sophisticated campaigns to implant advanced persistent threats on both civilian and government systems, including DOD. These campaigns can enable adversaries to maintain a covert presence on infrastructure networks, secrete malware designed to disrupt grid operations, and conduct other malicious activities to prepare for possible attacks on critical system components.[7] To frame such efforts more bluntly, adversaries are *preparing the battlefield* to create massive blackouts and other interruptions of critical services whenever they deem the moment right.

Adversaries recognize the foundational importance of grid-provided power for mission assurance and will target U.S. electric companies accordingly. Cyber attacks on the grid in Ukraine in 2015 and 2016 demonstrated key threat vectors that might be employed against U.S. utilities. In these cyber-induced blackouts, attackers crossed a key threshold: they moved cyberwarfare against electric systems from theory to (limited, but still unprecedented) practice. In 2015, attackers hijacked the grid's own operating systems to disconnect critical substations, creating brief but wide-area outages. Attackers were also able to "brick"[8] operating system components and communications devices.[9]

The 2016 event displayed even more sophisticated capabilities. After mapping the grid's operating systems, attackers used the system's own incident command system (ICS) protocols to open circuit breakers, creating blackouts.[10] The malware was unusually difficult to detect and included a wiper module that could brick grid control system components on a large scale.[11] Attackers also had the ability to deny or corrupt situational awareness data, making the grid extremely prone to cascading failures.[12]

Potential adversaries are conducting "test drives" of additional ways to attack the grid and other critical infrastructure that defense installations depend on. The Dragonfly campaign, which is still ongoing today, enables adversaries to use utility vendors and other trusted third parties to conduct attacks on targeted systems.[13] Triton malware (in use since at least September 2017) enables adversaries to corrupt the safety systems that monitor and protect the performance of key system components, creating new pathways for adversaries to sabotage and intentionally mis-operate critical infrastructure.[14] Most recently, the Department of Homeland Security (DHS) reported that Russian cyber campaigns have granted them access to utility human-machine interfaces and information on accessing ICS systems.[15] Adversaries can use these interfaces—and potentially ICS systems—to shut down or mis-operate portions of the grid.

These demonstrated adversary capabilities fail to represent the true scale and severity of the threat confronting the U.S. grid and the MEFs that depend on the flow of grid-provided power. Russia, China, North Korea, and other potential adversaries have powerful incentives to hold their most destructive cyber weapons in reserve; doing so helps hobble U.S. efforts at building protections against such weapons.

Recent studies by the Department of Energy (DOE), other governmental departments, and cyber experts in academia and the private sector highlight a range of potential cyber threats that these adversaries might use to cause outages far more severe than in Ukraine. Most concerning is the potential for adversaries to compromise operator workstations or use native ICS communication protocols to intentionally mis-operate grid components.[16] Adversaries could also significantly magnify the effect of cyber-induced outages by disabling the protection systems in place to safeguard the integrity of the grid; corrupting or denying state estimation and situational awareness capabilities; and wiping, overloading, or holding "ransom" critical components or systems.[17] In the future, adversaries that employ artificial intelligence to assist their attacks will increase the potential for damage and make defense against such strikes increasingly difficult.[18]

Implications for Mission Assurance Initiatives. The severity of cyber threats to the power grid and electricity-dependent infrastructure has far-reaching implications for MA policies and programs. Indeed, given the dependence of DOD force projection on civilian-operated ports, transportation assets, and other infrastructure, accelerating the restoration of grid-provided power will be of prime importance for mission assurance. This dependence on private infrastructure is not new. The U.S. military has long relied on civilian transportation and communications systems for operational logistics. However, adversaries are increasingly threatening this infrastructure as a means to disrupt and degrade U.S. warfighting capabilities. Building resilience against these threats will require new and deeper levels of collaboration with grid owners and operators.

One especially valuable focus of collaboration has been to improve the ability of defense installations to execute MEFs with emergency power. A growing number of defense installations are becoming capable of operating as "power islands," separated from the surrounding grid and able to serve critical loads with emergency generators, on-site fuel, and electricity distribution systems. These improvements are vital and must be sustained.

Emergency power capabilities, however, will be at increasing risk if adversaries create wide-area, long-duration power outages. In blackouts lasting more than a week, emergency power generators will start breaking down, and fuel resupply could become increasingly difficult to sustain. Moreover, many defense installations rely on grid-dependent infrastructure outside their perimeters (and beyond the reach of their emergency power systems). Installation personnel typically live in and commute from communities surrounding their bases. Water and wastewater systems, regional hospitals, and other supporting infrastructure that these personnel depend on will fail in long-duration outages. These disruptive effects will also cripple port operations and contractor-provided logistical systems essential to deploying and sustaining U.S. combat forces abroad. DOD MA initiatives should account for these risks and develop holistic strategies to support OPLAN execution.

Combined Cyber-Physical Threats and Additional Risks to Critical Infrastructure. Physical attacks on the grid add another threat vector for mission assurance. If adversaries can physically destroy large power transformers at critical substations in multiple states, they may be able to create exceptionally wide-area, long-duration outages, given the many weeks that will typically be required to transport and install replacement transformers. Such blackouts could have catastrophic effects on national security and public health and safety.

Electrical industry leaders have been increasingly concerned about the disruptive potential of kinetic attacks on grid infrastructure since the physical attacks on the Metcalf substation in April 2013. Fortunately, an adversary would face greater risks when launching physical rather than cyber attacks. Blowing up transformers and killing workers who are transporting replacement equipment might rapidly escalate conflict with the United States into larger scale kinetic warfare. In contrast to the typically less visible (and more difficult to detect) malware that cyber adversaries would hide on utility networks, arming and prepositioning covert teams to conduct physical attacks would also increase the risk that the United States would discover the attackers before they struck. Yet the potential rewards of physical attacks are immense, especially if the adversary believes that they will create power outages that last far longer than those induced by cyber weapons alone.

Unmanned aerial vehicles (UAVs) could also pose increasingly complex

First Security Forces Assistance Brigade Soldier uses Drone Defender with electromagnetic pulse to disable, capture, and control target drone, Camp Buehring, Kuwait, March 6, 2018 (U.S. Army/Brent Thacker)

kinetic threats. Improvements in drone technology and low-cost options increase the potential for adversaries to use UAVs to attack U.S. infrastructure, especially if they are equipped with improvised electromagnetic interference devices or other advanced payloads.[19] Even relatively simple UAVs can defeat traditional physical protections that focus on deterring or stopping armed personnel. Long-range drones could also present particular challenges for facilities overseas around which the United States does not control the airspace.

Even more concerning, however, is the threat that adversaries may launch combined cyber-kinetic attacks. The premier exercise system for the North American power grid, the GridEx series, is built around such combined threats because they could create multiweek power outages over multiple areas of the United States.[20] In particular, if adversaries can use physical attacks to destroy transformers and other critical electric infrastructure, and/or (potentially) deploy active shooters against utility employees once the attack is under way, the difficulty of defending the grid will be significantly greater than against cyber weapons alone.[21]

Electromagnetic pulse (EMP) attacks present another potentially catastrophic attack vector. The electric industry and its Federal partners are already strengthening preparedness against EMP attacks. For decades, DOD has taken measures to ensure the survivability of key communications systems and other defense assets against EMP threats. DOE and DHS have launched initiatives to help grid owners and operators protect their own systems against EMP effects.[22] Until recently, however, DOD has provided little support to electric utilities on hardening technologies and other protective measures, even though the disruption of power supplies in an EMP attack could significantly degrade the ability of defense installations to execute their MEFs.

Adversaries may also seek to incite public panic through social media and other information warfare operations to advance their broader political objectives. GridEx employs a threat scenario that includes combined cyber-kinetic attacks on power companies in multiple U.S. regions, as well as adversary information warfare campaigns on social media to disrupt restoration operations, inflame public fears, and create challenges for public messaging that are far more difficult to counter than in any past U.S. power outages. These disinformation operations could complicate efforts to provide defense support to civil authorities. They could also magnify the difficulty of ensuring that civilian employees for ports and other infrastructure

During loss of commercial power to Incirlik Air Base, Turkey, Airmen from 39th Logistics Readiness Squadron receive fuel from bladder off C-5M Super Galaxy, July 22, 2016 (U.S. Air Force/Caleb Pierce)

essential to MA continue to perform their functions.

Cross-Sector Interdependencies: A New Frontier for Mission Assurance. U.S. critical infrastructure sectors are becoming increasingly interdependent. These cross-sector dependencies are creating new risks of infrastructure failure and significant opportunities for adversaries to magnify the effects of their attacks on the power grid and other systems essential for MA. Accounting for this shift in the architecture of U.S. infrastructure will be essential for supporting OPLAN execution by U.S. defense installations.

The most immediate cross-sector risks to mission assurance lie in the interdependencies between natural gas transmission systems and the electric grid. A growing number of proposed DOD microgrids will rely on natural gas to fuel their generators. Moreover, in California, New England, and many other regions of the United States, gas provides an increasingly dominant source of fuel for generating grid-provided electricity for defense installations.

As natural gas has become an increasingly important fuel for electric generation, natural gas pipelines have also come to rely on electricity to function. Key components of gas pipeline systems, including the compressors and industrial control systems that keep gas flowing to power generators and other users, are more reliant on electric power. Adversary-induced outages could interrupt the flow of electricity to these components and (in a classic case of spiraling effects) magnify those outages by disrupting gas deliveries to power generators essential for power restoration.

MA initiatives will need to account for the risks created by these and other infrastructure interdependencies. It would be dangerously shortsighted to assume that gas-fired generators for DOD microgrids provide resilient power, without also ensuring the resilience of the natural gas pipelines that provide fuel for these generators. However, the potential for mutually reinforcing failures is not unique to the oil and natural gas subsector, and failures in other sectors could also threaten mission assurance. Equivalent challenges will exist for managing the risks posed by interdependencies between the grid and water systems, communications systems, and other tightly coupled infrastructure sectors. Public-private partnerships (P3s) focused on the electric industry and other sectors are necessary but not sufficient; to strengthen mission assurance, DOD will also need to conduct multisector risk analyses and mitigation initiatives.

Mission Assurance Abroad. For many CCDRs, especially in regional commands, executing OPLANs will require support from bases outside of the continental United States (OCONUS). Major U.S. bases in Europe, the Far East, and other areas depend on the same infrastructure services as installations in the United States. In particular, these bases depend on host-nation power grids to function (though they also typically have emergency power capabilities). Utilizing grid-provided power in OCONUS installations can significantly reduce energy costs. A comprehensive assessment of OCONUS base power options found that "in every case, it was found that bases connected properly to host nation power grids . . . would reduce the cost of energy for those bases, reduce fuel usage (and the associated logistic challenges), and increase base endurance. This was true even in cases where the host nation power grid had very low reliability." Accordingly, the study "strongly recommended that every U.S. military base consider using host nation power."[23]

Dependence on host-nation infrastructure services, however, carries significant risks. The July 2016 cutoff of power to a U.S. Air Force air base in Incirlik, Turkey, exemplifies these risks. Incirlik Air Base is essential for conducting U.S. military operations against the so-called Islamic State (IS), using manned and unmanned aircraft. The Turkish government cut off commercial electric power to Incirlik for nearly a week in 2016, following a failed coup attempt by members of the Turkish armed forces. A recent study of the event found that while the air base made use of standby generators, the Air Force was forced to reduce the number of sorties flown. Had the power outage continued, the Air Force would have had to stop flying altogether.[24] The bottom line: host nations can jeopardize mission assurance and OPLAN execution with a flip of the switch.

The foreign-owned infrastructure on which OCONUS installations depend is also vulnerable to the same cyber and kinetic threats that confront U.S. infrastructure. In Japan, for example, cyber threats from China, North Korea, and other potential adversaries are intensifying at least as rapidly as against the United States. However, Japan has been slower to buttress its cyber resilience.[25] Strengthening emergency power capabilities on U.S. installations will be essential to mitigate the risks of cyber attacks on host-nation infrastructure. DOD should also explore partnership opportunities to help strengthen the resilience of allied power grids.

Infrastructure interdependencies create additional challenges to U.S. mission assurance abroad. For U.S. installations in Europe, the dependence of local power generation on Russian-supplied natural gas provides a special threat. The Nord Stream-2 gas pipeline project will increase the leverage of Russia's Gazprom, which currently supplies around one-third of European Union gas. In 2009, Russia cut off gas supplies to Ukraine, with downstream consequences for the European Union. Amos J. Hochstein, U.S. Special Envoy and Coordinator for International Affairs, emphasizes that "our commitment to energy security in Europe is directly linked to our concern for national security."[26] That commitment must extend to strengthening mission assurance for U.S. installations reliant on Gazprom-fueled electricity generation.

Finally, China and other potential adversaries are buying up (and helping to operate) infrastructure around the globe, including in nations where U.S. defense installations support OPLAN execution. Chinese companies are rapidly increasing their investments in and ownership of foreign power and gas networks, buying assets in the United Kingdom, Spain, Australia, and Latin America.[27] These ownership and operation trends create an additional threat vector to manage and reinforce the need to bring OCONUS installations into the core of future mission assurance initiatives.

Recommendations

DOD is taking major steps to combat all the threats examined above. The analysis that follows offers recommendations on how DOD can ramp up that progress and expand the partnerships necessary to strengthen mission assurance.

Shifting the Paradigm: Mission Assurance as a Component of Warfighting. DOD Directive 3020.40 established an important policy shift by directing components to prioritize the CCMD execution of OPLANs. Focusing on OPLAN execution offers a range of potential benefits. By disaggregating OPLANs and identifying specific dependencies on installations, support functions, and the infrastructure that they rely on, DOD will be able to prioritize and target resilience initiatives in ways that produce the greatest value for deterrence and warfighting. Bolstering the resilience of Defense Critical Assets and other key components of well-established Defense Critical Infrastructure Protection (DCIP) programs will remain vital. However, additional measures will be necessary against adversaries who seek asymmetric means to degrade U.S. warfighting capabilities.

The Defense Department should move beyond outdated "tooth versus tail" debates over how to invest scarce resources and adopt a risk management approach to bolster end-to-end improvements in joint force lethality. In the past, DOD invested relatively little in ensuring the survivability of supporting infrastructure. That low priority made sense at the time; DOD could conduct warfighting abroad operations without concerns that adversaries would disrupt U.S. installations and the privately owned infrastructure systems that they depended on. In recent years, however, military bases in the United States have taken on increasingly important roles in conducting UAV operations and other warfighting and sustainment activities to execute CCMD OPLANs. As DOD dependence on U.S.-based installations has grown, adversaries have ramped up their ability to disrupt the flow of power and other critical infrastructure services that those bases rely on. Intelligent, adaptive adversaries will seek to defeat the United States without facing the point of its spear. Treating infrastructure resilience as a core warfighting requirement, and ensuring that adversaries cannot break the shaft of that spear, constitute an essential paradigm shift for mission assurance.

DOD should also intensify the focus of MA on supporting the execution of CCMD OPLANs. Combatant commanders must continue to ramp up their focus on the resilience of upstream assets and infrastructure, even if those assets are owned by others and lie outside their area of responsibility. Exercises can help support that transformation. Using severe but realistic scenarios to reflect the disruption of energy systems, transportation companies, and other infrastructure that near-peer adversaries can inflict, CCMDs and their partner components can assess potential effects on OPLAN execution. They can use these assessments to develop cost-effective options to address any MA shortfalls they identify.

Such reprioritization measures should be reflected in DOD budgeting systems. DOD leaders should examine a range of options to help build a culture of risk management that puts MA issues front and center in component and Department-wide investment and planning decisions, including:

- systematic efforts to remedy OPLAN-related MA shortfalls via the issue paper process
- use of the Joint Requirements Oversight Council system to strengthen MA
- modifications of the OPLAN development and review process to highlight (and develop options to mitigate) risks that adversaries will cripple OPLAN execution by striking essential installations and infrastructure.

In addition, DOD must develop MA strategies that better incorporate cross-cutting risks to MEFs, assets, and systems that span the domains of multiple Services and agencies. In the past, MA risk assessments too often focused on Service- or agency-specific concerns. Such narrow assessments cannot be simply aggregated to form a composite view of risks to OPLAN execution. A more joint (and more CCMD-led) approach will be crucial to counter asymmetric threats.

Finally, DOD must bring cybersecurity into the heart of mission assurance. The Department has made significant progress in moving beyond its traditional focus on "guns, guards, and gates" under DCIP and is accounting for a broader range of threats to mission assurance. DOD is also ramping up efforts to ensure that OPLANs can be executed even if cyber attacks disrupt the flow of grid-provided power to defense installations, ports, and the water systems and other infrastructure essential to their operations. DOD Instructions 8500.01, *Cybersecurity*, and 8510.01, *IT Risk Management Framework*, provide the policy foundations for these efforts. DOD Directive 3020.40 also emphasizes the need to integrate cyber issues into MA decisionmaking. However, the DOD catch-up process must accelerate to account for the growing severity and breadth of cyber challenges.

Expanding Partnerships with Critical Infrastructure Owners and Operators. Substantial policy support already exists for expanding P3s for both microgrids and accelerated power restoration for military bases. Both the 2012 MA strategy and DOD Directive 3020.40 emphasize the importance of partnering with the owners and operators of U.S. critical infrastructure, including the electric grid, to help ensure that the Department can perform its MEFs.

These policies have enabled the development of a growing number of P3s for installation microgrids as well as "outside the fence-line" initiatives to create redundant power feeds from the grid and other measures to strengthen the resilience of grid-provided power. DOD and its industry partners should continue to improve the ability of key defense installations to function as power islands segmented from the grid, with hardened on-site power generation, transmission, and distribution systems. DOD should also expand microgrid projects so that they can sustain service to water systems and other mission-critical loads in surrounding communities. Moreover, DOD and its industry partners should examine how these initiatives can be scaled up on a nationwide basis to help meet the intensifying cyber threat.

In addition to extending P3s for pre-event, steady-state collaboration and investments in grid resilience, DOD and industry need better plans and capabilities to coordinate operations in major events. A joint capacity for industry-government information-sharing will be a critical enabler. DOD should ensure that it has the appropriate mechanisms to receive data and malware threat signatures that these partners gather from operational technology logs (and vice versa), as well as assessments of potential risks to DOD-supporting infrastructure systems.

Industry and DOD have begun to consider enhancing such operational cooperation and coordination. During the GridEx IV exercise in November 2017, utility leaders expressed interest in exploring how the National Guard (operating in state Active-duty or full-time National Guard–duty [Title 32] status) might support state and local law enforcement and contractor security services to protect key substations and other grid assets from kinetic attack, including infrastructure that directly serves critical defense installations. Exercise participants and senior DOD leaders also discussed whether and how the National Guard might support utilities for post–cyber attack power restoration. DOD and its industry partners could further examine these cyber and physical security support options.

The private sector can also help DOD identify the specific critical assets and facilities that the Department depends on. The Federal Power Act provides the ideal point to move this effort forward. The act requires the Secretary of Energy, in consultation with other Federal agencies and grid owners and operators, to identify and designate "critical defense facilities" in the 48 contiguous states and the District of Columbia that are "(1) critical to the defense of the United States; and (2) vulnerable to a disruption of electric energy provided to such facility by an external provider."[28] Congress's definition of *defense critical electric infrastructure* also helps guide implementation of that requirement. Such assets include "any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary [of Energy]" as a critical defense facility, "but is not owned or operated by the owner or operator of such facility."[29]

DOD is already working with industry and DOE to identify defense critical electric infrastructure and the installations this infrastructure serves. DOD also has

South Carolina Army National Guardsmen from 228th Signal Brigade out of Spartanburg, South Carolina, set up Joint Incident Site Command Center package to support Horry County Emergency Operations Center with back-up communications system, September 15, 2018 (U.S. Army National Guard/ Brian Calhoun)

a well-established, continuously updated list of critical military bases and other DOD assets to support this identification process.[30] However, deterrence and power projection will also depend on sustaining electric service to a diverse array of ports, transportation systems, and other civilian-owned infrastructure.

DOD will therefore need industry-government partnerships outside the electricity subsector. MA initiatives must account for cross-sector infrastructure interdependencies, as adversaries can also disrupt other infrastructure sectors that defense installations depend on. Specifically, DOD needs to make greater progress in addressing the risks of cascading failures across other civilian-owned infrastructure sectors, including water utilities, natural gas pipelines essential for power generation, and transportation systems that MEFs may depend on.

Many of these sectors are rapidly improving their cyber defenses and adopting industry standards to ensure sector-wide compliance. However, ports and other infrastructure critical to MA have traditionally focused on physical security rather than cyber resilience. DOD can partner with port owners and operators to help them meet their cyber challenges. In addition to sharing appropriate information on potential threats, the Department can help these owners develop and adopt standardized policies for assessing, containing, and mitigating cyber risks.[31]

DHS recently announced creation of its National Risk Management Center (NRMC), which can play a centralizing role for coordination between DOD and both industry and government partners in all sectors. The NRMC will be a locus for industry-government collaboration on sector-specific and multisector risk management efforts, including prioritization initiatives.[32] As noted by Tom Fanning, chief executive officer of gas and electric utility Southern Company, the center could also help enable DOD and the Federal Bureau of Investigation to play a uniquely critical role in protecting U.S. critical infrastructure: "hold[ing] the bad guys accountable."[33]

Supply Chains as a Special Area of Focus. Supply chain risks offer a particularly important opportunity for collaboration between DOD and industry. Adversaries could disrupt the grid by corrupting widely used infrastructure components then exploiting those common vulnerabilities to cause massive breakdowns.[34] This threat applies to all critical infrastructure sectors. Software, firmware, hardware, or network services are all vulnerable to supply chain compromise, potentially enabling adversaries to inject destructive malware and/or gain access to sensitive components and data in utility systems. Foreign ownership of technology companies poses an increasing threat due to potential ties to adversarial governments, especially for infrastructure in countries abroad that house U.S. bases.[35]

DOD is already working to combat this threat. Ellen Lord, Defense Under Secretary for Acquisition and Sustainment, recently noted that the Pentagon has compiled a "do not buy" list of software, in close collaboration with the Intelligence Community, to protect against Russian and Chinese supply chain threats.[36] Senior DOD officials have also noted that the Department will start red-teaming suppliers and contractors to ensure their cyber defenses are sufficiently robust.[37] While DOD is making important progress for securing its own infrastructure supply chains, it needs to work with industry to share threat information and develop shared approaches. Significant industry-government collaboration could yield a number of benefits, including a reduction in the duplication of costs and the ability to create the market incentives sufficient to ensure effective implementation.

DHS is currently leading industry-government collaboration efforts to address supply chain threats. Supply chain risk management will be a key focus of NRMC.[38] The House Homeland Security Committee also recently approved HR 6430, *Securing the Homeland Security Supply Chain Act*, which would authorize the Secretary of Homeland Security to enact a wide range of measures to curb supply chain risks, including the exclusion of specific vendors to support "urgent national security interest[s]."[39] Given the intensifying threat to cyber supply chains and the potential for widespread damage if an adversary successfully compromises critical and widely shared system components, DOD leaders should ensure that the Department is actively working with its industry and government partners on this issue moving forward.

Mission Assurance Abroad. DOD leadership should expand risk management for mission assurance on a global basis. Thus far, mission assurance has focused primarily on installations and supporting infrastructure in the United States. However, many OPLANs also depend on support from U.S. bases located in partner nations. China and other potential adversaries are rapidly expanding their ownership of (or provision of key operational control systems for) critical infrastructure worldwide, creating a growing threat vector to U.S. defense facilities and functions abroad. DOD's Operational Energy Strategy and Installation Energy Instruction provide valuable starting points to help address these issues and strengthen mission assurance.[40]

The Department of Defense is making rapid progress to strengthen mission assurance. However, adversary capabilities to disrupt the infrastructure that DOD depends on is growing at least as quickly. By focusing mission assurance on supporting combatant command operational plan execution, and expanding partnerships with critical infrastructure owners and operators, the Defense Department can stay ahead of the threat and continue to improve joint force lethality in the face of these asymmetric threats. **JFQ**

This article could not have been written without the research and editorial assistance of Rob Denaburg, Director of Security Research & Analysis, Sonecon LLC.

Notes

[1] The Department of Defense (DOD) defines *mission assurance* as a "process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the performance of DOD MEFs [mission essential functions] in any operating environment or condition." See *Mission Assurance Strategy* (Washington, DC: DOD, April 2012), available at <http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf>.

[2] *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: DOD, January 2018), 3, available at <www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

[3] DOD defines *mission essential functions* as "Select functions directly related to accomplishing the Department's mission. Failure to perform or sustain these functions . . . would significantly affect the Department of Defense's ability to provide vital services or exercise authority, direction, and control." See DOD Directive 3020.26, *DOD Continuity Policy* (Washington, DC: DOD, February 14, 2018), available at <www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302026p.pdf>.

[4] *Mission Assurance Strategy.*

[5] DOD Directive 3020.40, *Mission Assurance* (Washington, DC: DOD, November 29, 2016), 3, available at <www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf>.

[6] Julian Barnes, "'Warning Lights Are Blinking Red,' Top Intelligence Officer Says of Russian Attack," *New York Times*, July 13, 2018, available at <www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html>.

[7] "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," U.S. Computer Emergency Readiness Team (U.S.-CERT), March 15, 2018, available at <www.us-cert.gov/ncas/alerts/TA18-074A>; "Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors," U.S.-CERT, October 20, 2017, available at <www.us-cert.gov/ncas/alerts/TA17-293A>; Defense Science Board (DSB), *Task Force on Cyber Deterrence* (Washington, DC: DOD, February 2017), 4, available at <www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf>; ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats* (Fairfax, VA: ICF International, June 2016), 19.

[8] *Bricking* a piece of equipment means rendering it unusable, often due to firmware that is damaged beyond repair. See "Bricking," *Techopedia*, available at <www.techopedia.com/definition/24221/bricking>.

[9] SANS Industrial Control Systems and Electricity Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case* (Washington, DC: SANS Industrial Control Systems and Electricity Sharing and Analysis Center, March 18, 2016), 2, available at <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf>.

[10] "Alert (ICS-ALERT-17-206-01): CRASHOVERRIDE Malware," SANS Industrial Control Systems Cyber Emergency Response Team, July 25, 2017, available at <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01>; "Alert (TA17-163A): CrashOverride Malware," U.S.-CERT, June 12, 2017, available at <www.us-cert.gov/ncas/alerts/TA17-163A>; *CRASHOVERRIDE: Analysis of the Threat to Electric*

Grid Operations, Dragos, Inc., June 13, 2017, 8, available at <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>; and DSB, *Task Force on Cyber Deterrence*, 4.

[11] "Alert (TA17-163A)."

[12] *CRASHOVERRIDE*, 24.

[13] "Alert (TA18-074A)."

[14] Andy Greenberg, "Unprecedented Malware Targets Industrial Safety Systems in the Middle East," *Wired*, December 14, 2017, available at <www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/>; Nicole Perlroth and Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," *New York Times*, March 15, 2018, available at <www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html>.

[15] Rebecca Smith, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," *Wall Street Journal*, July 23, 2018, available at <www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110>; "Alert (TA18-074A)."

[16] "Alert (TA18-074A)." Tim Conway, "Pictures and Theories May Help, but Data Will Set Us Free," SANS Industrial Control Systems, December 21, 2016, available at <https://ics.sans.org/blog/2016/12/21/pictures-and-theories-may-help-but-data-will-set-us-free>; Anton Cherepanov and Robert Lipovsky, "Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet," *WeLiveSecurity*, June 12, 2017, available at <www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>.

[17] Chris Sistrunk, "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)," SANS Industrial Control Systems, January 8, 2016, available at <https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one>; Anton Cherepanov, "Win32/Industroyer: A New Threat for Industrial Control Systems," *WeLiveSecurity*, June 12, 2017, 15, available at <www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf>; "Alert (TA17-163A)"; *Quadrennial Energy Review—Transforming the Nation's Electricity System: Second Installment of the QER* (Washington, DC: Department of Energy, January 2017); "Destructive Malware," SANS Industrial Control Systems Cyber Emergency Response Team, March 2017, 1, available at <https://ics-cert.us-cert.gov/sites/default/files/documents/Destructive_Malware_White_Paper_S508C.pdf>; "Alert (TA16-091A): Ransomware and Recent Variants," U.S.-CERT, September 29, 2016, available at <www.us-cert.gov/ncas/alerts/TA16-091A>.

[18] Greg Allen and Taniel Chan, *Artificial Intelligence and National Security* (Cambridge: Belfer Center for Science and International Studies, July 2017), 24, available at <www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf>.

[19] "Aerial Drones Present Increasing Threat to Critical Infrastructure," The Foundation for Resilient Societies, April 16, 2015.

[20] *Grid Security Exercise: GridEx III Report* (Atlanta, GA: North American Electric Reliability Corporation, March 2016), available at <www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.

[21] Paul W. Parfomak, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, R43604 (Washington, DC: Congressional Research Service, June 17, 2014), 2, available at <www.hsdl.org/?abstract&did=755610>.

[22] *U.S. Department of Energy Electromagnetic Pulse Resilience Action Plan* (Washington, DC: Department of Energy, January 2017); Brandon Wales, *Oversight of Federal Efforts to Address Electromagnetic Risks*, Testimony Before the U.S. House Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency, May 17, 2016, 3–4, available at <http://docs.house.gov/meetings/HM/HM09/20160517/104869/HHRG-114-HM09-Wstate-WalesB-20160517.pdf>.

[23] *Guidance for DOD Utilization of Host Nation Power* (Lexington, MA: MIT Lincoln Laboratory, October 2015), 5, available at <www.dtic.mil/get-tr-doc/pdf?AD=AD1034495>.

[24] Jeffrey Marqusee, Craig Schultz, and Dorothy Robyn, *Power Begins at Home: Assured Energy for U.S. Military Bases* (Reston, VA: Noblis, January 2017), 5, available at <www.pewtrusts.org/~/media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf>.

[25] Tim Kelly, "U.S. to Bring Japan Under Its Cyber Defense Umbrella," Reuters, May 30, 2015, available at <www.reuters.com/article/us-japan-us-cybersecurity/u-s-to-bring-japan-under-its-cyber-defense-umbrella-idUSKBN0OF0EL20150530>.

[26] "U.S. Deeply Concerned Nord Stream Gas Link Is Security Threat," Reuters, May 6, 2016, available at <www.reuters.com/article/us-eu-gazprom-us/u-s-deeply-concerned-nord-stream-gas-link-is-security-threat-idUSKCN0XX1YG>.

[27] Kane Wu and Clara Denina, "UK Power Reserve Sale Attracts China's State-Owned Grids—Sources," Reuters, September 29, 2017, available at <www.reuters.com/article/uk-power-m-a/uk-power-reserve-sale-attracts-chinas-state-owned-grids-sources-idUKKCN1C4292>.

[28] See 16 U.S.C. § 824o-1, *Critical Electric Infrastructure Security*, § (c), available at <www.law.cornell.edu/uscode/text/16/824o-1>.

[29] See also 16 U.S.C. § 824o-1, § (a)(4).

[30] DOD Manual 3020.45, *Defense Critical Infrastructure Program* (Washington, DC: DOD, May 23, 2017), available at <www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>; and DOD Directive 3020.40: *Mission Assurance* (Washington, DC: DOD, November 29, 2016).

[31] Daniel Trimble, Jonathon Monken, and Alexander F.L. Sand, "A Framework for Cybersecurity Assessments of Critical Port Infrastructure," in *2017 International Conference on Cyber Conflict* (Washington, DC, November 7–8, 2017), 1, available at <https://ieeexplore.ieee.org/document/8167506/>.

[32] "National Risk Management Center Fact Sheet," Department of Homeland Security, July 31, 2018, available at <www.dhs.gov/sites/default/files/publications/18_0731_cyber-summit-national-risk-management-fact-sheet.pdf>.

[33] Dustin Volz, "Pence Blames Russia for 2016 Election Interference, Vows to Tighten Cybersecurity," *Wall Street Journal*, July 31, 2018, available at <www.wsj.com/articles/dhs-forms-new-cyber-hub-to-protect-critical-u-s-infrastructure-1533029400>.

[34] *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, Mission Support Center Analysis Report (Idaho Falls: Idaho National Laboratory, August 2016), 20.

[35] *Foreign Economic Espionage in Cyberspace* (Washington, DC: National Counterintelligence and Security Center, July 2018), 12, available at <www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf>.

[36] Roxana Tiron, "Pentagon's 'Do Not Buy' List Targets Russian, Chinese Software," *Bloomberg*, July 27, 2018, available at <www.bloomberg.com/news/articles/2018-07-27/pentagon-s-do-not-buy-list-targets-russian-chinese-software>.

[37] Marcus Weisgerber and Patrick Tucker, "Pentagon Creates 'Do Not Buy' List of Russian, Chinese Software," *Defense One*, July 27, 2018, available at <www.defenseone.com/threats/2018/07/pentagon-creates-do-not-buy-list-russian-chinese-software/150100/>.

[38] "National Risk Management Center Fact Sheet."

[39] "DHS Sets New ICT Supply Chain Task Force," *MeriTalk*, July 31, 2018, available at <www.meritalk.com/articles/dhs-sets-new-ict-supply-chain-task-force/>.

[40] *Department of Defense 2016 Operational Energy Strategy* (Washington, DC: DOD, May 2016, available at <www.acq.osd.mil/eie/Downloads/OE/2016%20DoD%20Operational%20Energy%20Strategy%20WEBc.pdf>; and DOD Instruction 4170.11, *Installation Energy Management* (Washington, DC: DOD, March 16, 2016), available at <www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/417011p.pdf>.