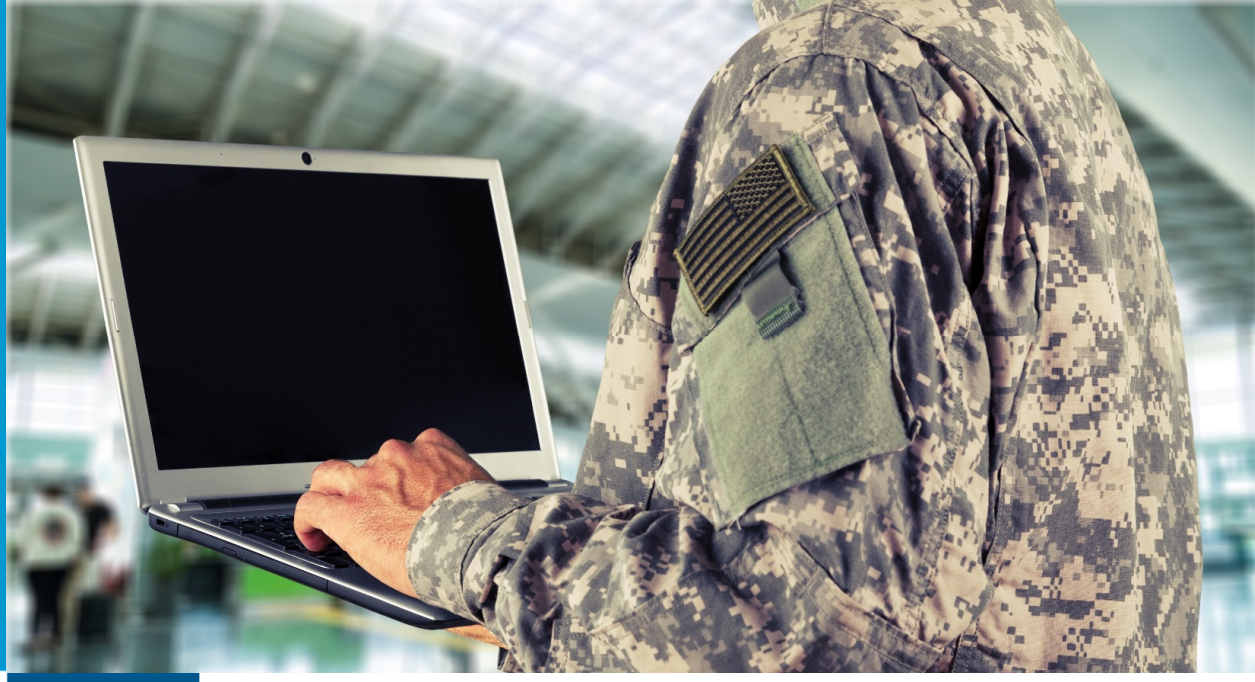


Strengthening Mission Assurance against Emerging Threats: Critical Gaps and Opportunities for Progress

U.S. Combatant Commanders 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 at home and abroad require electric power and other infrastructure support, typically provided by U.S. civilian-owned utilities or host nation assets. 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 DOD has taken far-reaching measures to strengthen mission assurance (MA).[1] In particular, DOD has expanded on its traditional emphasis on the Defense Critical Infrastructure Program (DCIP) and is adopting a more holistic and integrated appro ach to support OPLAN execution by regional and functional Combatant Commanders (CCDRs). 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 power, water, ports, and other support functions. Private sector infrastructure owners and operators are also increasingly concerned that adversaries will combine cyberattacks 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 may jeopardize mission execution.

Dr. Paul Stockton
in collaboration with
Colonel John Paczkowski, USMCR (Ret.)

February 16, 2018

[1] DOD defines mission assurance (MA) 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 in any operating environment or condition.” See: Department of Defense, *Mission Assurance Strategy*, April 2012, http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf.

Staying ahead of these threats will require continued progress in reframing stakeholder perspectives on mission assurance. Individual services and agencies will remain vital for building the resilience of their critical assets. However, Combatant Commands (CCMDs) will have a broader, multi-service understanding of the facilities and functions that will be critical to executing their operational plans, and can champion the integrated assessment of asymmetric threats and establish priorities to mitigate them.

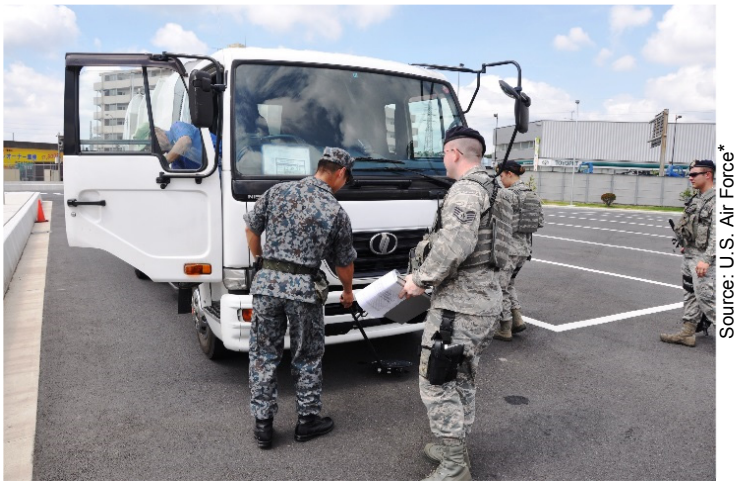
DOD and its public and private sector partners can help assure the execution of OPLANS and bolster force lethality and resilience by accelerating progress in four realms. We will examine each of these opportunities more closely in the analysis that follows.

I. Strengthen the culture of mission assurance by focusing on the execution of CCMD OPLANS. DOD has long prioritized tooth over tail; investments in supporting facilities and critical infrastructure and have suffered accordingly. Given the risk that adversaries will attack such infrastructure to disrupt OPLAN execution, a paradigm shift is essential. CCMDs must continue to ramp up their focus on the resilience of upstream assets and infrastructure, even if those assets are privately-owned and lie outside their Area of Responsibility (AOR). Senior DOD leaders should continue to build a culture of risk management that puts MA issues front and center in component and department-wide investment and planning decisions. DOD leaders should also consider specific options to address investment shortfalls via issue papers, the Joint Requirements Oversight Council (JROC) system, and the OPLAN development and review process.

II. Bring cybersecurity into the heart of mission assurance. DOD has made significant progress in moving beyond its traditional focus on "guards, guns, and gates" under the DCIP, and is accounting for a broader range of threats to mission assurance. In particular, while the *Mission Assurance Strategy* (April 2012) barely mentioned cyber challenges, DOD Directive 3020.40, *Mission Assurance* (November 2016) emphasizes the need to integrate cyber issues into MA decision-making. But DOD's catch-up process must accelerate to account for the growing severity and breadth of cyber challenges. This study highlights the nature of these challenges to the power grid and infrastructure that supports Defense installations and their Mission Essential Functions, including disruption or exploitation of industrial control systems (ICS), supply chains and other key DOD interdependencies. The study also identifies options to strengthen mission assurance against the emerging threat environment, and suggests key topics for further examination by the Office of the Secretary of Defense, the Joint Staff, and the CCMDs.

III. Cross-sector infrastructure interdependencies. DOD is vastly better positioned to provide resilient power for OPLAN execution than a decade ago, when *More Fight, Less Fuel* revealed the vulnerabilities created by DOD's dependence on the grid (DSB, 2008). However, 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 on which MEFs may depend – especially if adversaries simultaneously attack multiple infrastructure sectors.

IV. Mission assurance abroad. 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. The cut-off of power to the Incirlik Air Force Base in July 2016 highlighted the additional risk that host countries may halt critical infrastructure



Source: U.S. Air Force*

DCIP is expanding its focus to fully examine inter-dependencies and risks over the fence line beyond the guns, guards, and gates of perimeter security.

* Senior Airman Katrina R. Menchaca, 120806-F-JZ010-861.JPG

services (CNN, 2016). DOD's Operational Energy Strategy and Installation Energy Instruction provide valuable starting points to help address these issues and strengthen mission assurance (DOD, 2016a; DOD, 2016c). This paper provides recommendations on how to build on that foundation, and expand risk management for MA on a global basis.

I. EMERGING THREATS TO MISSION ASSURANCE: THE IMPERATIVE FOR CYBERSECURITY

No comprehensive, unclassified overview of the threat to mission assurance yet exists. As a starting point to develop such an overview, and to prioritize and frame recommendations to strengthen MA, the analysis that follows highlights key features of the emerging threat.

This analysis begins with the most immediate and formidable challenge to mission assurance: the risk of cyberattacks on the electric power grid and other civilian-owned infrastructure on which Defense operations depend. This section also examines the risk that adversaries will conduct hybrid warfare operations against such infrastructure, and combine cyberattacks with targeted kinetic strikes and information operations to cripple the restoration of electric power and other defense-critical services.

A. Cyberattacks on the Grid and Other Supporting Infrastructure

The Trump Administration's National Security Strategy notes that cyber weapons "enable adversaries to attempt strategic attacks against the United States – without resorting to nuclear weapons – in ways that could cripple our economy and our ability to deploy our military forces" (President Trump, 2017, p. 27).

DOD is taking major steps to meet these cyber challenges, and is strengthening the resilience of Defense assets (including platforms and on-base industrial control systems) against increasingly sophisticated adversary capabilities. DOD Instructions on Cybersecurity (8500.01) and an IT Risk Management Framework (8510.01) provide the policy foundations for these efforts. DOD is also ramping up efforts to ensure that OPLANS can be executed even if cyberattacks disrupt the flow of grid-provided power to DOD installations, ports, and the water systems and other infrastructure essential to their operations.

A key area of focus has been to improve the ability of DOD installations to execute their MEFs with emergency power. A growing number of DOD 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.

However, emergency power capabilities 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 DOD 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 on which these personnel depend 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.

Adversaries recognize the foundational importance of grid-provided power for mission assurance, and will target U.S. electric companies accordingly. In 2015 and 2016, cyberattacks on the grid in Ukraine demonstrated key threat vectors that might be employed against utilities in the United States. However, those capabilities represent only the tip of the iceberg in terms of the capabilities that Russia, China, and other potential adversaries will be able to employ to disrupt the flow of electricity to U.S. Defense facilities and functions, and to the distribution of power within military bases.

1. Proof of Concept Attacks in Ukraine

In the cyber-induced blackouts of 2015 and 2016, attackers crossed a key threshold: they moved cyberwarfare against electric systems from theory to (limited, but still impressive) practice. The 2015 attack demonstrated the effectiveness of two particularly important threat vectors. First, attackers in the 2015 event used the grid's own operating systems to disrupt

electric service. After gaining remote access to the utility control networks, attackers hijacked human-machine interfaces (HMIs) to disconnect critical substations from the grid, creating brief but very wide-area outages. Second, attackers used KillDisk malware and malicious firmware updates to "brick" operating system components and communications devices (SANS ICS and E-ISAC, 2016, p. 2). We should expect that adversaries will exploit these threat vectors against U.S. power companies as well, by intentionally misoperating[2] the grid and destroying system components that provide power to Defense installations.

The 2016 Ukraine blackout demonstrated even more sophisticated capabilities. Attackers installed CrashOverride malware to carefully map the grid's operating systems, and then, using the system's own ICS protocols, opened circuit breakers to create blackouts (ICS-CERT, 2017a; US-CERT, 2017a; Dragos, 2017, p. 8; and DSB, 2017, p. 4). CrashOverride malware is unusually difficult to detect, and includes a wiper module that can brick grid control system components on a large scale (US-CERT, 2017a). Adversaries could also use CrashOverride modules to prevent grid operators from understanding the status of their own systems, and show breakers as closed when they are actually open (Dragos, Inc., 2017, p. 24). Such measures to deny or corrupt situational awareness could make the grid extremely prone to cascading failures, particularly when adversaries are using cyberattacks to intentionally misoperate the grid.

2. Beyond Ukraine: The Attacks to Come

Over the past few months, potential adversaries have conducted "test drives" of additional ways to attack the grid and other critical infrastructure on which Defense installations depend. 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 (US-CERT, 2017b). 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 misoperate critical infrastructure (Wired, 2017).

However, these demonstrated adversary capabilities fail to represent the true scale and severity of the threat confronting the U.S. grid. 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 government 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. Emerging threat vectors include the following:

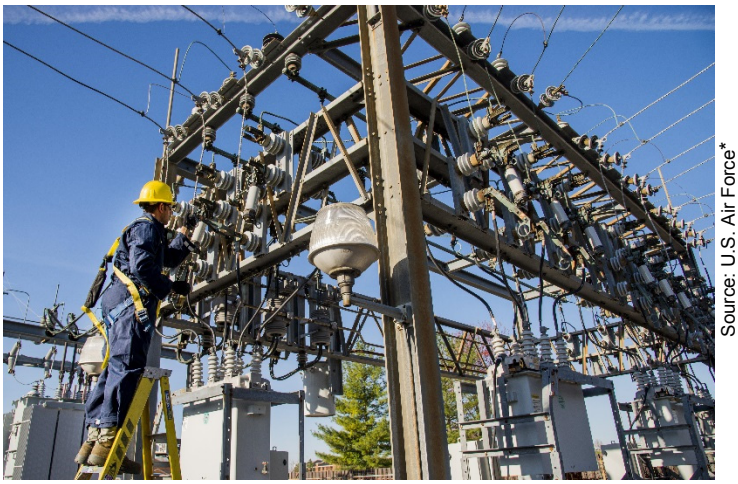
- ***Supply Chain Corruption.*** Adversaries could disrupt the grid by corrupting widely used grid components, then exploiting those common vulnerabilities to cause massive breakdowns. Infrastructure owners and operators often find it difficult to ensure the integrity of their supply chain (INL, 2016, p. 20). 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. This is particularly concerning for industry standard grid components that are used by many utilities across the United States, creating the potential for one threat actor to trigger extremely widespread failures.
- ***Attacks on Protection Systems.*** Attacks on the systems in place to safeguard the integrity of the grid and protect key components from power surges have the potential to be particularly catastrophic. Protective relays that isolate faults to protect equipment and stem cascading power failures are indeed prime targets for adversary exploitation. While these relays were once

[2] Grid owners and operators are familiar with the concept of misoperation, as defined in the North American Electric Reliability Corporation's (NERC's) glossary (see: "Glossary of Terms Used in NERC Reliability Standards," *NERC*, last updated January 2, 2018, http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf). The glossary refers to failures or deficiencies in a specific class of grid components—protective systems. The concept of intentional misoperation, used throughout this analysis, differs in two ways. First, intentional misoperation is indeed deliberate, whereas NERC's definition implies unintended malfunctioning. While the latter is not benign, it is materially less threatening than a capable adversary's strategic campaign to disrupt power flows. Second, NERC's narrow focus on protection systems ignores the wider array of grid components that have the potential to be intentionally misoperated in a way that can cause grid failures. Intentional misoperation of grid components is likely a new standard for cyberattacks on the grid.

electromechanical, much of the grid now relies on microprocessor-based relays that are vulnerable to cyberattacks (SANS ICS, 2016a). Some attacks may attempt to take these relays offline (ESET, 2017, p. 15; and US-CERT, 2017a), leaving the system vulnerable to equipment damage and cascading failures unless and until relays can be manually reset. Other attacks may intentionally misoperate the relays to induce such failures. Inadvertent misoperation of these relays "continues to be one of the largest contributors to the severity of transmission outages" (NERC, 2017b, p. 2). If adversaries intentionally target relays for disruption, and can also cause power surges to flow across U.S. transmission systems, damage to grid components could be severe.

- ***Intentional Misoperation of Other Grid Components.*** The 2007 "Aurora" test at the Idaho National Laboratory provided an early proof of concept for the ability to remotely misoperate and physically damage power generators (NERC, 2010, p. 32). Since that test, efforts have been underway to remediate the vulnerabilities that Aurora demonstrated. Those efforts need to continue. In addition, however, new potential attack vectors are also emerging, including the following:
  - ***Operator Control Systems.*** Adversaries can cause severe outages by compromising operator workstations and using them to send malicious commands to grid control systems. Adversaries have exhibited the ability to gain access to devices that utility operators use to control grid components and may be able to do so without any visible indication to that operator (SANS ICS, 2016c). Adversaries may seek to attack far more U.S. substations than occurred in the 2015 HMI-based attacks on Ukraine, and may also specially design those attacks to create cascading failures.
  - ***Industrial Control Protocols for Grid Operation.*** Future U.S. adversaries may also use communication protocols native to the components themselves to directly induce malicious changes, and do so on a vastly greater scale and sophistication than occurred in the 2016 Ukraine attack. These protocols are the backbone of ICS operations, communicating actions to physical components of the grid to control the flow of power. Moreover, these protocols were designed decades ago, without any considerations for cybersecurity. Attackers, therefore, do not necessarily have to find 'vulnerabilities' within the protocols; they simply need embed the protocol language into the malware to potentially cause "cascading failures and … serious damage to equipment" (ESET Blog, 2017). These challenges are all the greater because many utilities lack the situational awareness and monitoring capabilities to detect attacks targeted deep into control system protocol stacks.

Experts have identified potential cyber threats that could cause widespread national grid outages severely impacting mission critical operations.



Source: U.S. Air Force*

- ***Load Manipulation.*** An entirely new threat vector has emerged, due in part to the modernization of the grid. While threat assessments often focus on generation and transmission assets, power flows from these potential targets represent only half of the load-generation balance required for grid stability. A drastic change in load could also lead to instability and power swings, causing outages and equipment damage. Digital smart meters (also known as advanced metering infrastructure), which are increasingly replacing their analog predecessors to improve accuracy and energy efficiency, provide a prime example. Some meters have the ability to be switched off remotely (DOE, 2016, p. 20). If adversaries gain access to large

* Airman Daniel Garcia, 160409-F-SH665-967.JPG
The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

numbers of these smart meters, they could potentially cause "a widespread blackout by switching smart meters on and off repeatedly" (POLITICO, 2017). While DOE emphasizes the importance of cybersecurity for advanced metering infrastructure (AMI) (DOE, 2016, p. 69), recent studies suggest advanced cyberattacks against AMI remain "a clear and present danger" (Hansen et. al, 2017, p. 3).

- ***Attacks on State Estimation.*** Adversaries could significantly amplify the destructive effects of a cyberattack on critical electric infrastructure by disabling or corrupting state estimation capabilities. Operating the grid depends on constant situational awareness through real-time assessments of system conditions and contingency analysis. System-generated alerts based on these state estimations are "the fundamental means by which system operators identify events on the power system that need their attention" (UCPSOTF, 2004, p. 52). A malfunction in one such system was a significant contributing factor to cascading power failures across the northeastern United States in the August 2003 blackout. Grid operators are developing fallback systems to manage power flows in the absence of state estimation inputs. Nevertheless, the potential for adversaries to corrupt situational awareness data during a disruptive cyberattack, delaying corrective actions or cause operators to take or refrain from taking actions that could harm the system, remains a threat. Given the speed at which failures propagate, a successful attack on state estimation to obfuscate the effects of a disruptive cyberattack could contribute to multi-region cascading failures.
- ***Distributed Denial of Service (DDoS) Attacks.*** Adversaries could also target critical infrastructure components with DDoS attacks to exacerbate the disruptive effects of a cyberattack, and/or amplify restoration challenges. The growing Internet of Things has led to a massive proliferation of network connectivity in traditionally not-connected objects and devices, many of which are insufficiently secured. Adversaries have demonstrated their ability to compromise large numbers of these devices, harnessing them in a botnet to overwhelm Internet-connected targets with web traffic (DOE, 2017a, p. 7-3). Networked system control components may be vulnerable to DDoS attacks, meaning that botnets could play a direct role in causing major grid instability. An adversary could also use a DDoS attack to disable key components in other critical infrastructure sectors, including communications systems vital to power restoration, as part of a larger cyber campaign against the grid.
- ***Data Wiping.*** Beyond the capabilities witnessed in the Ukraine attacks, adversaries will likely attempt to debilitate electric utilities by using data wiper modules to disable information and control systems. Wiper malware is deployed to destroy large amounts of data or effectively brick targeted systems (ICS-CERT, 2017b). The 2012 attack on Saudi Aramco, for example, wiped 30,000 Windows-based computers, but did not affect industrial control systems (Reuters, 2012). More recent attacks, however, have included wiper modules that target control systems and networks. Future attacks may infect and effectively brick thousands of control system components, though doing so is not likely to cause infrastructure outages on its own. Disabling supervisory control and data acquisition (SCADA) systems adds risk and complicates grid operations, but will not interrupt power flows without some external form of disruption (SANS ICS, 2016b). Moreover, electric utilities are increasingly planning for the loss of SCADA functionality, and are upgrading their current capabilities to operate the grid manually in the event that control systems are degraded or have failed entirely (FERC-NERC, 2017, p. 4). Advanced adversaries could nonetheless deploy wiper modules to compound and exacerbate lasting effects in the aftermath of a more complex attack, and delay restoration by forcing infrastructure operators to manually operate portions of the grid.
- ***Ransomware.*** Ransomware attacks are an increasingly concerning threat vector for critical infrastructure information systems. Much like data wiping malware, ransomware threatens to render computers inoperable. Ransomware infects a computer system and restricts users' access or encrypts the computer's contents, forcing the user to pay a fee to unlock the screen or access their own files (US-CERT, 2016). This malware can often exploit vulnerabilities to move laterally

through a network, infecting as many endpoints as possible (ICS-CERT, 2017c). Once infected, the only way to restore functionality requires the user to pay a ransom (for each individual machine) to an adversary attacking the grid, or an actor launching the attack on their behalf. Otherwise, all infected endpoints must be replaced.

While recent attacks (WannaCry, Petya/NotPetya, etc.) have been expansive in reach, they did not present a particularly disruptive threat to the grid. However, more advanced ransomware attacks have the potential to infect – and potentially act as a vector to intentionally misoperate – industrial control systems. In a mock attack, researchers were able to gain access and then send commands to programmable logic controllers in a simulated water plant, and warned that these tactics are the "next logical step" for ransomware attacks (Georgia Tech, 2017). Such an advanced form of ransomware attack has yet to occur, or at least be acknowledged publicly. However, as adversaries continue to improve their offensive capabilities, the use of ransomware to disrupt utility operations and restoration efforts present a significant growing threat.

- ***Artificial Intelligence.*** Over the longer term, adversaries may use Artificial Intelligence (AI) to assist their attacks, and make real-time defense against them much more difficult. AI tools may enable adversaries to automate labor-intensive functions currently performed by highly skilled cyber personnel, lowering the human capital required to map U.S. utility infrastructure and control systems, design sophisticated attacks, and strike the grid in a comprehensive way. Once attacks are underway, adversaries may also be able to use AI to help detect and maneuver around our defensive measures, and do so at a "machine-speed" that overmatches human decision-making (Belfer Center, 2017, p. 24). China has declared its intention to become the world leader in AI and is committed to applying its expertise to "leapfrog" U.S. Defense capabilities (CNAS, 2017, p. 4). Russia is also ramping up its AI research and development efforts. U.S. power companies and their government partners will need to respond accordingly, and accelerate the consideration of grid protection measures against AI-enabled attacks.

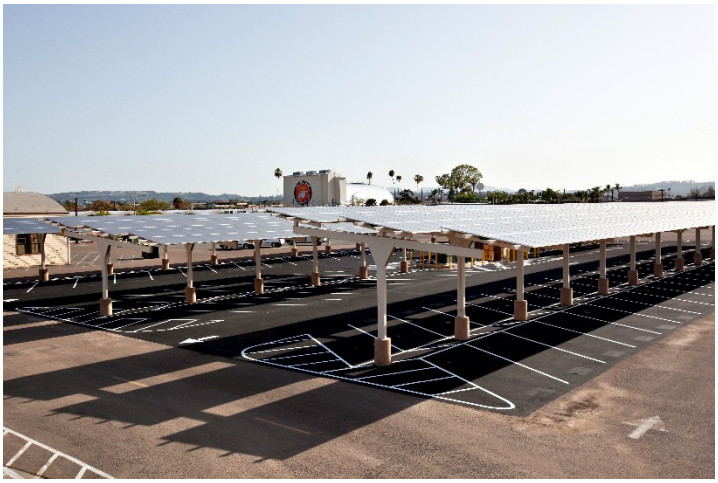
3. Implications for Mission Assurance Initiatives

The severity of cyber threats to the power grid and electricity-dependent infrastructure has far-reaching implications for MA policies and programs. DOD and its electric industry partners should continue to improve the ability of key Defense installations to function as power islands segmented from the grid, with on-site power generation, transmission, and distribution systems hardened against all of the threats examined above. Over time, DOD should also expand these microgrids so that they can sustain service to water systems and other mission-critical loads in surrounding communities.

However, 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 MA. Achieving that goal will require new and deeper levels of collaboration with grid owners and operators.

Substantial policy support already exists for expanding public-private partnerships (P3s) for both microgrids and accelerated power restoration for military bases. DOD's *Mission Assurance Strategy* (2012) emphasizes the importance of partnering with the owners and operators of U.S. critical infrastructure, including the electric grid, to help ensure that DOD can perform its Mission Essential Functions (DOD, 2012, p. *i* and pp. 16–19). A key follow-on document, DOD Directive 3020.40, *Mission Assurance* (November 2016), further specifies that military departments and other DOD components should "partner with non-DoD entities, as appropriate and permitted by law," to help ensure that DOD installations can carry out their critical missions (DOD, 2016b, p. 4).

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. The DOD mission assurance community needs to examine how these initiatives can be scaled up on a nationwide basis to help meet the intensifying cyber threat.



Source: MCAS Miramer NREL 18238

DOD policies are enabling microgrid installations to create redundant power feeds to strengthen installation resilience and mission assurance.

B. Hybrid Warfare: Additional Threats to the Power Grid and Other Key Sectors

The National Security Strategy notes that in addition to cyberattacks, the vulnerability of U.S. critical infrastructure to "physical and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication" (President Trump, p. 12).

Electric 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. 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 multi-week power outages over multiple areas of the United States (NERC, 2017a; and NERC, 2016a). 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 underway, the difficulty of defending the grid will be significantly greater than against cyber weapons alone (CRS, 2014, p. 2; NERC, 2015).

Fortunately, the ability to launch coordinated physical attacks across the United States lies beyond the reach of many cyber-armed adversaries. Nations with the requisite capabilities may be deterred from employing kinetic strikes because of the risk that the United States will discover their covert forces before they attack. Adversaries may also believe that if they conduct physical attacks on the U.S. homeland, versus using only cyber weapons, U.S. leaders will be more likely to respond with overwhelming force (especially if adversaries believe that they can launch cyberattacks without being identified as the source).

Nevertheless, the risks of attacks targeting grid infrastructure are sufficiently severe that NERC has established mandatory protection standards for both cyber and physical threats to the Bulk Power System (BPS), which is comprised of the power generators, high voltage transmission systems, and other infrastructure necessary to operate and maintain the reliability of North America's interconnected electric systems.[3] Though NERC's definition of the BPS does not broadly include distribution facilities, distribution providers that own assets critical to grid reliability are specifically required to comply with NERC's cybersecurity regulations (NERC, 2016b).

Despite these standards, a lack of coordination between industry and DOD poses an unaddressed risk to mission assurance. NERC standard CIP-002-5.1a (*Cyber Security – BES Cyber System Categorization*) categorizes grid cyber systems as high, medium, or low impact, and assigns to each category "cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES" (NERC, 2016b). However, DOD and infrastructure owners and operators are still in the process of cross-referencing the cyber assets and associated facilities that serve DOD installations with

[3] NERC uses the definition from Section 215 of the Federal Power Act, defining the BPS as "facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy." NERC, *Memorandum: Use of "Bulk Power System" versus "Bulk Electric System" in Reliability Standards*, April 10, 2012, http://www.nerc.com/files/final_bes_vs%20_bps_memo_20120410.pdf.

this categorization scheme. It is therefore possible that DOD facilities rely on transmission substations and/or generation units that are required to comply with only the minimum regulatory standards for cybersecurity and, as a result, are potentially more vulnerable. Coordination between DOD and industry officials will be necessary to eliminate this risk, and would provide an immediate opportunity to strengthen MA.

DOD and its electric industry partners have already expressed interest in enhancing 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 DOD installations. Exercise participants and senior DOD leaders also discussed whether and how the National Guard might support utilities for post-cyberattack power restoration. The proposed MA conference could provide opportunities to discuss these cyber and physical security support options.

The electric industry and its Federal partners are also strengthening preparedness against Electromagnetic Pulse (EMP) attacks. For decades, DOD has taken measures to ensure the survivability of key communications systems and other DOD assets against EMP. The Department of Energy (DOE) and the Department of Homeland Security (DHS) have launched initiatives to help grid owners and operators protect their own systems against EMP effects (DOE, 2017b; and Wales, 2016, pp. 3-4). 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 DOD installations to execute their MEFs.

Of course, cyber, physical, and EMP threats can also disrupt other infrastructure sectors on which DOD installations depend. These multi-sector-sector threats are intensifying against bases not only in the United States but also abroad. Sections IV and V of this study examine multi-sector and outside of the continental United States (OCONUS) challenges to MA. First, however, it will be helpful to analyze the broader opportunities to strengthen DOD's culture of MA, and the implications for bringing cyber resilience into the heart of the MA-related policies, programs, and budgeting.

II. SHIFTING THE PARADIGM: MISSION ASSURANCE AS A COMPONENT OF WARFIGHTING

The issuance of DOD Directive 3020.40, *Mission Assurance* (November 2016) marks a major step forward in implementing DOD's 2012 *Mission Assurance Strategy* (DOD, 2016b; and DOD, 2012). The Directive remedies a key gap in the 2012 Strategy by integrating cybersecurity issues into MA. The Directive strengthens DOD-wide governance and coordination mechanisms for MA. Especially valuable, the document directs DOD components to prioritize MA efforts to help fulfill critical DOD strategic missions, including CCMD's execution of OPLANS (DOD, 2016b, p. 3).

Focusing on OPLAN execution offers a range of potential benefits. First, by disaggregating OPLANS and identifying specific dependencies on installations, support functions, and the infrastructure on which they rely, 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 programs will remain vital. However, against adversaries who seek asymmetric means to degrade U.S. warfighting capabilities, ensuring that the CCMDs can execute their OPLANS *regardless* of attacks on supporting infrastructure will help take a potentially catastrophic threat vector off the table.

Progress toward achieving that goal has been limited, and may soon fall behind the rapidly intensifying threats of cyberattack and hybrid warfare against U.S. infrastructure. Three deeply entrenched constraints on DOD decision-making continue to hobble such progress.

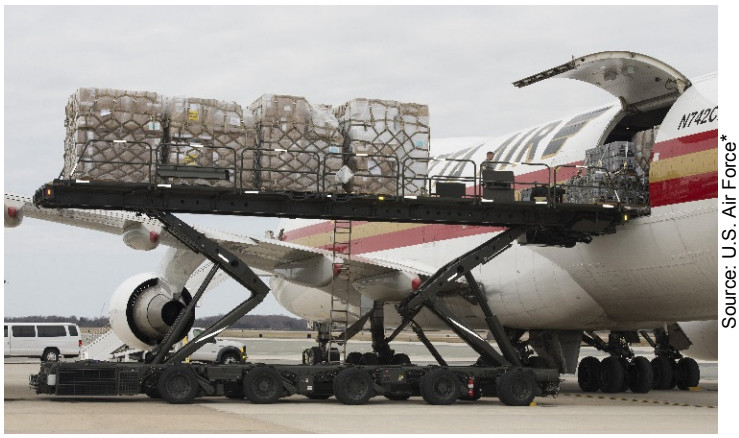
First, as noted in the introduction, DOD has long prioritized tooth over tail. Investments in strengthening the resilience of supporting infrastructure and facilities have suffered accordingly. That low priority made sense in past decades; DOD could conduct warfighting operations with less reliance on U.S. installations and the privately owned infrastructure on which they depend. In recent years, however, military bases in the United States have taken on increasingly important roles in conducting unmanned aerial vehicle (UAV) operations and other warfighting and sustainment activities to execute CCMD OPLANS. As DOD's dependence on U.S. installations has grown, adversaries have ramped up their ability to disrupt the flow of power and other critical infrastructure services on which those bases rely. Intelligent, adaptive adversaries will seek to defeat us without facing the point of our spear. Treating infrastructure resilience as a core warfighting requirement, to ensure that they cannot break the shaft of that spear, constitutes a paradigm shift that is essential to accelerate.

Second, DOD budgeting systems and priorities remain tied to the past preeminence of tooth over tail. Again, while those priorities fit the needs of past decades, new approaches will be required to enable the execution of CCMD OPLANS in the face of asymmetric adversary strategies to disrupt mission-essential installations and supporting infrastructure. A concerted effort is needed to advance a range of options to help DOD leaders build a culture of risk management that puts MA issues front and center in component and DOD-wide investment and planning decisions. These include the following:

- Systematic efforts to remedy OPLAN-related MA shortfalls via the Issue Paper process;
- Use of the JROC system to strengthen MA; and
- 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.

Third, until recently, DOD was relatively autonomous in supporting and conducting combat operations. While DOD depended on the Defense Industrial Base to develop and manufacture weapons and provide other Defense materials and services, the private sector played only a limited role in assuring the ability of CCMDs to execute their OPLANS. That era is over.

USTRANSCOM relies heavily on commercial air, ground, and maritime transportation partners who are vulnerable to energy disruptions or cyberattack.



Source: U.S. Air Force*

U.S. Transportation Command (USTRANSCOM) missions exemplify the growing degree to which privately owned and operated systems (across multiple transportation sector subcomponents) are absolutely vital to DOD. Chinese cyberattacks on key USTRANSCOM contractors also highlight the risk that adversaries will disrupt CCMD missions by disrupting DOD's private sector partners (Senate Committee on Armed Services, 2014).

P3s are now absolutely essential to sustain the flow of electricity and other critical infrastructure services in the face of emerging threats. Treating P3 initiatives accordingly, and developing new mechanisms that enable DOD to expand them across the United States, will be essential.

Finally, risks to mission essential functions, assets, and systems are often cross-cutting in nature and span the domains of multiple services and agencies. In the past, however, MA risk assessments too often focused on service- or agency-specific concerns. Such narrow assessments cannot be simply aggregated together 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.

* Senior Airman Zachary Cacicia, 170324-F-BF216-1071.JPG

III. 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 potential cascading effects, thus posing 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 infrastructure protection will be essential to supporting OPLAN execution by DOD installations and networks.

The most immediate cross-sector risks to MA 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. Gas pipeline systems need compression pumps to sustain the flow of gas. Historically, these compressors were fueled with gas taken from the pipelines themselves. However, in many regions of the United States, these compressors are being replaced by variable speed electric-powered units to reduce on-site methane emissions and increase compressor efficiency. Adversary-induced outages could interrupt the flow of electricity to these units, and (in a classic case of spiraling effects) magnify those outages by disrupting gas deliveries to power generators essential for power restoration.

Some compression stations do have emergency power generators and at least some on-site fuel to sustain operations in a blackout. However, as noted above, fuel resupply operations for these stations will be at risk of catastrophic disruption in long duration, wide-area outages. These growing interdependencies create risks of cascading, mutually reinforcing failures across both the electricity and oil and natural gas energy subsectors (EIS Council, 2016). A significant interruption of the supply of natural gas can start a chain of events that result in interruption of electricity, which can cause the loss of power to gas compressors, which can cause further interruptions of generator fuel supply, cascading toward a broader system outage. The result: *gas and electric systems will be vulnerable to mutually reinforcing failures when such outages begin.*

MA initiatives will need to account for the risks created by these infrastructure interdependencies. Imagining 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, would be dangerously shortsighted. 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. Indeed, equivalent challenges will exist for managing the risks posed by water system-grid interdependencies and other tightly coupled infrastructure sectors. P3s focused on the electric industry and other sectors are necessary but not sufficient; to strengthen MA, DOD will also need to

Cyber attacks on natural gas generation and distribution systems could create cascading failures across the electrical energy subsector, as well as downstream effects on mission critical DoD assets.

conduct multi-sector risk analyses and mitigation initiatives.

IV. MISSION ASSURANCE ABROAD

For many CCMDs, especially in Regional Commands, executing OPLANS will require support from bases 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 stated 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" (MIT Lincoln Laboratory, 2015, p. 5).

However, dependence on Host Nation infrastructure services carries significant risks. The July 2016 cutoff of power to a U.S. Air Force base in Incirlik, Turkey exemplifies these risks. Incirlik Air Base is essential for conducting U.S. military operations against ISIS, using manned and unmanned aircraft. The Turkish government cut off commercial electric power to Incirlik Air Base 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 (Marqusee et al., 2017). The bottom line: Host Nations can jeopardize MA 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 (Reuters, 2015). Strengthening emergency power capabilities on U.S. installations will be essential to mitigate the risks of cyberattacks 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. MA 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 a third of the European Union's (EU's) gas. In 2009, Russia cut off gas supplies to Ukraine, with knock-on effects for the EU. Amos Hochstein, U.S. special envoy and coordinator for international affairs, emphasized that "Our commitment to energy security in Europe is directly linked to our concern for national security" (Reuters, 2016). That commitment must extend to strengthening MA for U.S. installations reliant on Gazprom-fueled electricity.

Finally, China and other potential adversaries are buying up (and helping to operate) infrastructure around the globe, including in nations where DOD 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 (Reuters, 2017). 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 MA initiatives.

BIBLIOGRAPHY

Belfer Center for Science and International Affairs (Harvard Kennedy School). Greg Allen and Taniel Chan. *Artificial Intelligence and National Security*. July 2017. https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf.

Center for a New American Security (CNAS). Elsa B. Kania. *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*. November 2017. https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235804.

CNN. Barbara Starr. "Turkey's power cutoff to Incirlik Air Base a problem for Pentagon." July 19, 2016. http://www.cnn.com/2016/07/19/politics/incirlik-air-base-turkey-failed-coup-power-cutoff/index.html.

CNN. Gregory C. Allen. "Putin and Musk are right: Whoever masters AI will run the world." September 5, 2017. https://www.cnn.com/2017/09/05/opinions/russia-weaponize-ai-opinion-allen/index.html.

Congressional Research Service (CRS). Paul W. Parfomak. "Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations (R43604)." June 17, 2014.

Defense Science Board (DSB). *Task Force on Cyber Deterrence*. February 2017.

Defense Science Board (DSB) Task Force on DoD Energy Strategy. *More Fight, Less Fuel*. February 2008. https://www.dau.mil/policy/PolicyDocuments/the1090Final%20Report%20of%20the%20DSB%20Task%20Force%20on%20DoD%20Energy%20Strategy%20%20Tab%20B.pdf.

Department of Defense (a). *2016 Operational Energy Strategy*. May 2016. http://www.acq.osd.mil/eie/Downloads/OE/2016%20DoD%20Operational%20Energy%20Strategy%20WEBc.pdf.

Department of Defense (b). *Department of Defense Directive 3020.40: Mission Assurance*. Effective November 29, 2016. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf.

Department of Defense (c). *Department of Defense Instruction 4170.11: Installation Energy Management*. Effective March 16, 2016. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/417011p.pdf.

Department of Defense. *Department of Defense Instruction 8500.01: Cybersecurity*. March 14, 2014. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf.

Department of Defense. *Department of Defense Instruction 8510.01: Risk Management Framework (RMF) for DoD Information Technology (IT)*. Effective July 28, 2017. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf.

Department of Defense. *Mission Assurance Strategy*. April 2012. http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf.

Department of Defense. *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*. January 2018.

Department of Energy. *Advanced Metering Infrastructure and Customer Systems*. September 2016.

Department of Energy (a). *Quadrennial Energy Review – Transforming the Nation's Electricity System: Second Installment of the QER*. January 2017.

Department of Energy (b). *U.S. Department of Energy Electromagnetic Pulse Resilience Action Plan*. January 2017.

Dragos, Inc. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*. June 13, 2017.

Dunford, General Joseph F. *Remarks and Q&A at the Center for Strategic and International Studies*. Washington, DC. March 29, 2016. http://www.jcs.mil/Media/Speeches/Article/707418/gen-dunfords-remarks-and-qa-at-the-center-for-strategic-and-international-studi/.

Electric Infrastructure Security (EIS) Council. *Handbook II (Vol 1 – Fuel)*. July 18, 2016. http://www.eiscouncil.com/App_Data/Upload/149e7a61-5d8e-4af3-bdbf- 68dce1b832b0.pdf.

ESET. Anton Cherepanov. *Win32/Industroyer: A new threat for industrial control systems*. June 12, 2017.

ESET Blog: WeLiveSecurity. Anton Cherepanov and Robert Lipovsky. “Industroyer: Biggest threat to industrial control systems since Stuxnet.” June 12, 2017. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC). *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans – Further Joint Study: Planning Restoration Absent SCADA or EMS (PRASE)*. June 2017. https://www.ferc.gov/legal/staff-reports/2017/06-09-17-FERC-NERC-Report.pdf.

Georgia Tech. John Toon. “Simulated Ransomware Attack Shows Vulnerability of Industrial Controls.” February 13, 2017. http://www.news.gatech.edu/2017/02/13/simulated-ransomware-attack-shows-vulnerability-industrial-controls.

Hansen, Aaron, Jason Staggs and Sujeet Shenoi. “Security analysis of an advanced metering infrastructure.” *International Journal of Critical Infrastructure Protection*, Vol. 18. (September 2017): 3-19.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (c). “Alert (ICS ALERT-17-181-01C) Petya Malware Variant (Update C).” Last revised July 10, 2017. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-181-01C.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (a). “Alert (ICS-ALERT-17-206-01): CRASHOVERRIDE Malware.” July 25, 2017. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (b). *Destructive Malware*. March 2017.

Idaho National Laboratory (INL). *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*. August 2016.

Lawfare, Elsa Kania. “Great Power Competition and the AI Revolution: A Range of Risks to Military and Strategic Stability.” September 19, 2017. https://www.lawfareblog.com/great-power-competition-and-ai-revolution-range-risks-military-and-strategic-stability.

Marqusee, Jefffrey, Craig Schultz and Dorothy Robyn. *Power Begins at Home: Assured Energy for U.S. Military Bases*. January 2017. http://www.pewtrusts.org/~/media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf.

MIT Lincoln Laboratory. *Guidance for DoD Utilization of Host Nation Power*. October 2015. www.dtic.mil/get-tr-doc/pdf?AD=AD1034495.

National Institute of Standards and Technology (NIST). *Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security*, Revision 2. May 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

North American Electric Reliability Corporation (NERC) (b). *CIP-002-5.1a – Cyber Security – BES Cyber System Categorization*. Effective December 27, 2016. http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber%20Security%20—%20BES%20Cyber%20System%20Categorization&jurisdiction=United%20States.

North American Electric Reliability Corporation (NERC). *CIP-014-02 – Physical Security*. Adopted May 7, 2015. http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf.

North American Electric Reliability Corporation (NERC) (a). *Grid Security Exercise: GridEx III Report*. March 2016. http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf.

North American Electric Reliability Corporation (NERC) (a). “GridEx.” 2017. http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx.

North American Electric Reliability Corporation (NERC). *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*. June 2010.

North American Electric Reliability Corporation (NERC) (b). *State of Reliability 2017*. June 2017.

POLITICO. Anca Gurzu. “Hackers threaten smart power grids.” January 11, 2017, http://www.politico.eu/article/smart-grids-and-meters-raise-hacking-risks/.

President Donald J. Trump. *National Security Strategy of the United States of America*. December 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Reuters. "Exclusive: Insiders suspected in Saudi cyber attack." September 7, 2012. https://www.reuters.com/article/net-us-saudi-aramco-hack/exclusive-insiders-suspected-in-saudi-cyber-attack-idUSBRE8860CR20120907.

Reuters. "U.S. deeply concerned Nord Stream gas link is security threat." May 6, 2016. https://www.reuters.com/article/us-eu-gazprom-us/u-s-deeply-concerned-nord-stream-gas-link-is-security-threat-idUSKCN0XX1YG.

Reuters. "U.S. to take Japan under Cyberdefense Umbrella as Hacker Threats Grow." May 31, 2015, https://www.japantimes.co.jp/news/2015/05/31/national/politics-diplomacy/u-s-to-bring-japan-under-cyberdefense-umbrella/#.Wj_gXVWnGUl

Reuters. "UK Power Reserve sale attracts China's state-owned grids – sources." September 29, 2017. https://www.reuters.com/article/uk-power-m-a/uk-power-reserve-sale-attracts-chinas-state-owned-grids-sources-idUKKCN1C4292.

SANS Industrial Control Systems (ICS) (a). Chris Sistrunk. "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)." January 8, 2016. https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one.

SANS Industrial Control Systems (ICS) (b). Michael J. Assante. "Confirmation of a Coordinated Attack on the Ukrainian Power Grid." January 9, 2016. https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.

SANS Industrial Control Systems (ICS) (c). Tim Conway. "Pictures and Theories May Help, but Data Will Set Us Free." December 21, 2016. https://ics.sans.org/blog/2016/12/21/pictures-and-theories-may-help-but-data-will-set-us-free.

SANS Industrial Control Systems (ICS) and E-ISAC. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. March 18, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Senate Committee on Armed Services. *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors*. 2014. https://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf.

U.S.-Canada Power System Outage Task Force (UCPSOTF). *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. April 2004.

US-CERT. "Alert (TA16-091A): Ransomware and Recent Variants." Last updated September 29, 2016. https://www.us-cert.gov/ncas/alerts/TA16-091A.

US-CERT (c). "Alert (TA17-132A) Indicators Associated With WannaCry Ransomware." Last updated May 19, 2017. https://www.us-cert.gov/ncas/alerts/TA17-132A.

US-CERT (a). "Alert (TA17-163A): CrashOverride Malware." June 12, 2017. https://www.us-cert.gov/ncas/alerts/TA17-163A.

US-CERT (d). "Alert (TA17-181A): Petya Ransomware." Last revised July 28, 2017. https://www.us-cert.gov/ncas/alerts/TA17-181A.

US-CERT (b). "Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors." October 20, 2017. https://www.us-cert.gov/ncas/alerts/TA17-293A.

Wales, Brandon. "Oversight of Federal Efforts to Address Electromagnetic Risks." *Testimony Before the United States House of Representatives Committee on Homeland Security Subcommittee on Oversight and Management Efficiency*. May 17, 2016. http://docs.house.gov/meetings/HM/HM09/20160517/104869/HHRG-114-HM09-Wstate-WalesB-20160517.pdf.

Wired. Andy Greenberg. "Unprecedented Malware Targets Industrial Safety Systems in the Middle East." December 14, 2017. https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/.

Dr. Paul N. Stockton

Paul Stockton is the Managing Director of Sonecon, LLC, a security and economic advisory firm in Washington, DC. Before joining Sonecon, Dr. Stockton served as the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In that position, he was responsible for Defense Critical Infrastructure Protection and led the creation of the Department's first-ever Mission Assurance Strategy. Dr. Stockton served as DOD's Domestic Crisis Manager and was responsible for Defense continuity of operations. He was the principal civilian advisor to the Secretary of Defense for providing Defense support to the Federal Emergency Management Agency and DHS in Superstorm Sandy, Hurricane Irene, and other disasters. Dr. Stockton also served as the Executive Director of the Council of Governors and was responsible for developing and overseeing the implementation of DOD security policy in the Western Hemisphere.

Dr. Stockton was twice awarded the Department of Defense Medal for Distinguished Public Service, DOD's highest civilian award. The Department of Homeland Security awarded Dr. Stockton its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. In 2016, he authored *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System*, Johns Hopkins University Applied Physics Laboratory; *Electric Grid Protection Handbook II: Water Sector Resilience for Black Sky Events,* Electric Infrastructure Security Council (ISBN 978-0-9971659-0-6); and co-authored the Homeland Security Advisory Council's *Final Report by the Cybersecurity Subcommittee: Incident Response.*

Dr. Stockton serves on the Homeland Security Advisory Council for Secretary of Homeland Security Kirstjen Nielsen and is a member of the Board of Directors of Analytic Services, Inc., the Strategic Advisory Council of the Idaho National Laboratory (INL), the INL Science and Technology Committee, and the Center for Cyber and Homeland Security Studies, George Washington University. Dr. Stockton also serves as a Senior Fellow of the Johns Hopkins University Applied Physics Laboratory.

Colonel John P. Paczkowski, USMCR (Ret.)

John Paczkowski is Senior Vice President for Homeland Security and National Resilience at ICF, a global policy, technology, and management advisory services firm. At ICF he directs a range of infrastructure security and resilience, emergency management, and risk mitigation services for local, state, and federal agencies, the DOD, and the private sector. Following a key leadership role in response to and recovery from the 9/11 attacks on the World Trade Center complex in New York, he was appointed Director for Emergency Management and Security at the Port Authority of New York and New Jersey. In that role he led corporate security, disaster preparedness, and risk mitigation programs and was the chief architect of a $1 billion risk-based security capital investment program.

In 2008 he was named a Distinguished Fellow by the Center for Homeland Defense and Security at the Naval Postgraduate School and since then has been a subject matter expert with the Center's Senior Leaders Seminar. In 2010, he was named a Senior Fellow at George Washington University's Center for Cyber and Homeland Security where he currently serves on the Advisory Board supporting homeland security related research initiatives. Mr. Paczkowski is past Chairman of the Security Analysis and Risk Management Association and a former member of the Board of Directors for the Infrastructure Security Partnership, sponsored by the Society of American Military Engineers.

In 2005, Mr. Paczkowski completed 33 years of active and reserve service as a Colonel in the U.S. Marine Corps. A former infantry and combat engineer officer, his service included key homeland defense leadership posts, with his final tour being Chief, Civil Support Branch, Domestic Operations at the National Guard Bureau. He holds a BS in Industrial Engineering and MS in Engineering Management from the New Jersey Institute of Technology, an MA in Organizational Psychology from Columbia University, and an MA in Security Studies from the Naval Postgraduate School.