Electrical Energy Overreliance

A Marine Corps vulnerability

by Capt Sharon Rollins

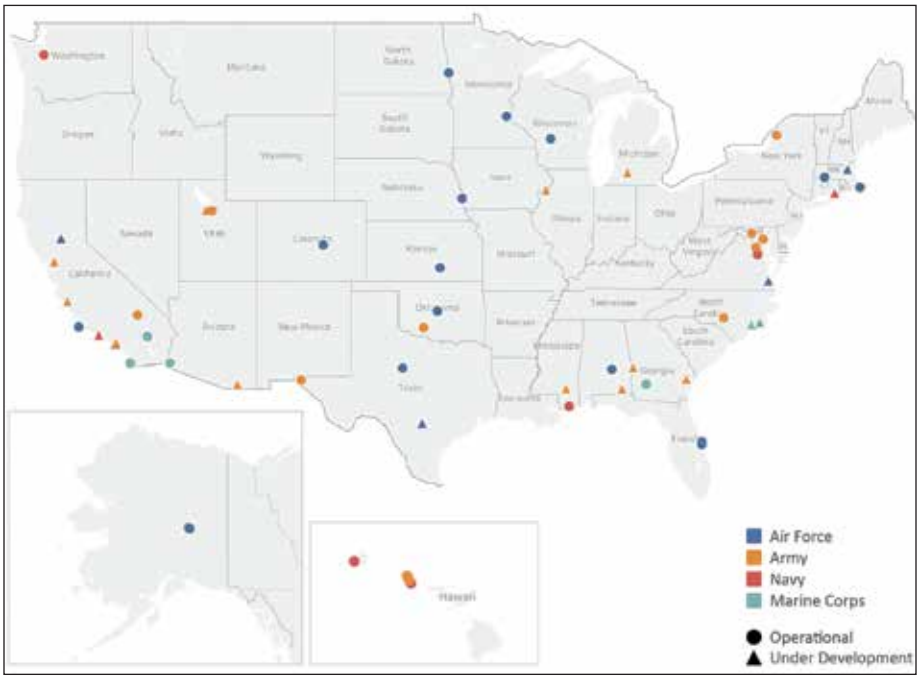
Imagine a scenario where Marine Corps Base Camp Lejeune instantly loses power, communications, and utilities supporting the majority of the installation—silence and panic fill the base as security levels rise. It is identified that an advanced Russian hacking unit burrowed into the commercial utility network and gained access to the power plant's critical controls that manage the base. First inaudible fires, second audible fires—how does the Marine Corps respond? In 2018, the Department of Homeland Security and Federal Bureau of Investigation released reports detailing efforts by the Russian government to target critical American infrastructure networks, particularly within the energy sector.[1] The reports describe this scenario and indicate that "China, Iran and North Korea are actively strengthening cyber capabilities to target critical infrastructure."[2] Nearly 99 percent of over 500 DOD installations nationwide are dependent on commercial power grids.[3] Marine Corps command and control (C2), logistics, medical, and millions of households are interdependent on one critical requirement: energy. Enemies seek to target this critical requirement in order to expose a vulnerability; therefore, the Marine Corps needs to accelerate and prioritize efforts in support of installation energy resiliency. Key members tasked and successful in increasing operational energy resiliency will ensure the Marine Corps remains relevant and survivable. To counter cyber or electromagnetic threats, and natural disasters, the Marine Corps needs to expedite hardening of installation infrastructure, increase contested environment training, and promote energy resiliency to ensure relevancy and sustainability in the future battlefield.

>Capt Rollins is a 1702 Cyberspace Officer. She is currently assigned to Marine Corps Cyberspace Warfare Group, Fort Meade, MD.

One problem with overreliance on public electrical grids is the threat of cyber-attacks. The 2018 DOD Annual Report to Congress: *Military and Security Developments Involving the People's Republic of China* states,

> Chinese People's Liberation Army (PLA) writings note the effectiveness of cyber warfare in recent conflicts and advocate targeting an adversary's C2 and logistics networks to affect its ability to operate during the early stages of conflict.[4]

Furthermore, PLA focuses on cyber-attacks against enemy C2 systems with potential to "completely disrupt" these systems, paralyzing the victim and thus gaining battlefield superiority.[5] The report's key findings conclude by stating China is "committed to building a more capable PLA that can fight jointly; harness real-time, data-networked C2 and precision strike; and operate increasingly far away from China's shores."[6] Cyber threats are today's reality, and



Association of Defense Communities, Beyond the Fence Line: Strengthening Military Capabilities Through Energy Resilience Partnerships, (Washington, DC: Association of Defense Communities, 2018), available at https://www.defensecommunities.org. *(Photo courtesy of Converge Strategies, LLC.)*

the Marine Corps should make sure its infrastructure security, training, and protocols are in place in case of an attack. It is crucial that the Marine Corps is not reactionary in response to the increasing cyber threat—especially in relation to operational energy.

In addition to the cyber threat, adversaries have developed and enhanced nuclear weapons. The doomsday nuclear threat is arguably unlikely by some; however, nuclear weapons have evolved to range the full electromagnetic spectrum. An electromagnetic pulse (EMP) is a super-energetic radio wave triggered by natural, cyber, nuclear, or frequency means that can damage or destroy electronic systems, power grids, frequency, and satellite communications. Other methods of inaudible fires, sonic, or waveform-based weapons are increasingly inexpensive to create. Russia, China, North Korea, and Iran possess the capability and have incorporated EMP attack into their military doctrine. They view nuclear EMP as "the ultimate cyber weapon" used either alone or in coordination with other methods of attack.[7] The civilian sector acknowledges the threat, and many organizations have added redundant energy sources in an effort to harden systems and critical information. The *Small Wars Journal* states,

> In this world of flux and constant pursuit of competitive advantage, by far and away the most disruptive technologies will be tactical level EMP weapons.[8]

The Marine Corps is not equipped to handle an EMP attack; it will cripple installation C2 and cause friction, chaos, and disorder for which Marines are unprepared.

Lastly, damage because of natural disasters are an increasing threat to installations. Severe flooding and destructive high winds impacted Camp Lejeune in 2017 with damages reaching $3.6 billion, and the base is still not completely recovered.[9] The 2018 Fourth National Climate Assessment states,

> Extreme weather events are expected to increasingly disrupt our Nation's energy and transportation systems, threatening more frequent and longer-lasting power outages, fuel shortages, and service disruptions, with cascading impacts on other critical sectors.[10]

Many Marine Corps buildings are outdated and not equipped to withstand continued natural disaster damage. During the rebuild of Camp Lejeune and the renovation of other bases, it is critical that the Marine Corps plan for an energy resilient infrastructure.

Strategic policy exists that enforces energy efficiency within the DOD ...

Strategic policy exists that enforces energy efficiency within the DOD, but actions at the operational level need improvement. The Department of Energy (DOE) ensures military readiness by pursuing energy security and resilience. Because of Federal assessments of commercial power grid vulnerability, the Assistant Secretary of Defense for Energy, Installations, and Environment said DOD continues "development of distributed energy sources which can be used to power critical missions regardless of the condition of the commercial grid."[11] *DOD Instruction 4170.11, Installation Energy Management*, (Washington, DC: December 2009), reinforces DOE's policy into a more specific strategy, and local installation energy plans execute in accordance with the DOD Instruction. Services were required to complete the majority of installation energy plans in fiscal year 2019 (FY19).[12] It is critical that Marine Corps Installations Command (MCICOM) work with the U.S. Navy and key agencies like—DOE and Marine Forces Cyberspace Command—in building resilient energy installation plans. A thorough assessment of installation energy resiliency will identify and resolve infrastructure, network, training, and policy vulnerabilities in the event of an attack impacting electrical power.

A unified task force consisting of industry and academia experts from the DOD, DOE, Office of Naval Research, MCICOM, Marine Corps Expeditionary Energy Office (E2O), Marine Forces Cyberspace Command, Massachusetts Institute of Technology, joint services, and local gas and electric companies should assess and develop

2018–A tree collapsed outside 2d Battalion, 2d Marines, during Hurricane Florence, on MCB Camp Lejeune. Hurricane Florence impacted Camp Lejeune and MCAS New River with destructive winds, flooding and storm surges resulting in major damages and power outages. ***(Photo by LCpl Isaiah Gomez, www.marines.mil).***

thorough installation energy plans to improve Marine Corps energy resiliency. After identifying current protocols and processes and conducting detailed planning, the task force would simulate attacks (cyber, EMP, or natural disaster) targeting installation energy. External third-party penetration tests (pen tests) are authorized cyber-attacks performed to assess vulnerabilities and strengths of a network, ultimately identifying recommendations for improvement. Additionally, controlled environment electrical power outages have the ability to assess an installation's continuity of operations plan and disaster recovery plan by means of verifying C2, training, and operational responsiveness. These controlled "pull the plug" exercises would eliminate power in critical buildings and test responsiveness, operability, and recovery from the mass outage. Assessments could compare installations that currently do and do not employ redundant power sources and have developed contested environment training plans. For example, Marine Corps Air Ground Combat Center (MCAGCC) Twentynine Palms, Marine Corps Air Station (MCAS) Miramar, and MCAS Iwakuni employ alternative solar and microgrid technology, but most remaining installations do not. When the MCAS or MCAGCC electrical grid is degraded or denied, the microgrid or solar systems supporting critical infrastructure serve as a form of redundant power until primary sources are restored. The primary source of power could be restored in hours or weeks; meanwhile, critical systems are powered via alternative means. This is an example of a small step in the right direction, although there is more work to be done. As a result of the assessments, installation continuity of operations plan and energy plans would determine vulnerabilities and redundant energy sources to invest in, training in a contested environment would be enhanced, defense of the Marine Corps enterprise network would be enhanced, and policy and processes would be further developed. Execution is key, starting with energy resiliency assessments.

If the Marine Corps was required to complete installation energy plans in FY19, a unified task force should be assembled now to assess and improve installation energy resiliency against cyber or electromagnetic threats and natural disasters. Addressing vulnerabilities, developing training, and investment and construction of redundant energy sources will take time. A timeline by 2030 for every installation to employ redundant power in support of critical buildings will ensure the Marine Corps is prepared and equipped to confront threats and respond aggressively. As far as Service branches are concerned, the Navy and Marine Corps fall behind the energy readiness of the Army and Air Force. Thus, the proposed Marine Corps task force should coordinate with and access the plans of sister Services in order to solve this joint problem.

Fortunately, sister Service actions can serve as a model to emulate. The Massachusetts Military Asset and Security Strategy Task Force held an annual Defense Energy Roundtable in 2018 focused on enhancing energy resilience at installations in Massachusetts (MA) and brought together DOD, public, research, and innovation leaders. U.S. Army and Air Force leaders discussed how they have pulled the plug on some of their bases, effectively cutting off electricity as a way to test responsiveness, recovery, and resume missions:[13] "MA is home to the first cyber-secure microgrid in the country at Joint Base Cape Cod," said MA Clean Energy Center Chief Executive Officer, Stephen Pike.[14] A Marine Corps representative was not in attendance at

When the MCAS or MCAGCC electrical grid is degraded or denied, the microgrid or solar systems supporting critical infrastructure serve as a form of redundant power until primary sources are restored.

2019–National Renewable Energy Laboratory (NREL) researcher Kate Anderson meets with USA COL Wortlinger, Fort Carson, CO garrison commander, at the base's utility scale lithium ion Battery Energy Storage System (BESS) installation. NREL provided an independent review of Fort Carson's proposed BESS through funding from the U.S. Department of Energy's Federal Energy Management Program. NREL verified the batteries' potential economic savings and helped Fort Carson characterize technology risk. ***(Photo by Dennis Schroeder/NREL–www.nrel.gov.)***

2019-NREL researcher Kate Anderson and the Fort Carson garrison commander, COL Wortlinger, review a photovoltaic (PV) array damaged by hail. Fort Carson was hit with a record hail storm, resulting in damage to 25–50 percent of the PV systems on site. Through funding from the U.S. Department of Energy's Federal Energy Management Program, NREL evaluated long-term safety and performance issues, developed lessons learned on how to address damage, and developed guidelines on how to evaluate contractor solutions. ***(Photo by Dennis Schroeder/NREL–www.)***

this meeting, but the Marine Corps could implement lessons learned via the aforementioned unified task force. Currently, there is no installation-level training to improve energy resilience and operations in powerless or energy contested environments. The right team assessing Marine Corps installations by conducting controlled energy-contested exercises, in addition to pen tests, will identify current power, network, and operational vulnerabilities as a result of cyber or electromagnetic threats and natural disasters. Applying pressure during training facilitates growth, and installations that identify weaknesses, will improve as a result.

A counterargument to this problem is that "someone else" is already assessing installation energy resiliency (a contractor, U.S. Navy, MCICOM, or the E2O). A task force would be wasted time and money when an entity is already doing this. However, installation energy plans need to be a unified, joint effort with multiple key agencies, not a collateral billet or contracted responsibility. Installation security and resiliency need to be an active priority against current threats and capabilities. Other counterarguments are, "bases already have backup generators" in the event of a power outage, or that "a mass outage effecting the entire base is unlikely." While many installations maintain backup fuel generators as a means of redundant energy, an actively engaged task force would assess and provide feedback regarding the "backup generator plan" in support of the installation energy plan. Lastly, there is not a current example of a mass electrical outage aboard a U.S. military installation as a result of a cyber or EMP attack. To assume that a most dangerous course of action will not happen goes against basic Marine Corps doctrine. The *Marine Corps Planning Process* states:

> One of the most important aspects covered in the adversary's intentions is the identification and discussion of his most likely and most dangerous courses of action.[15]

A defensive mindset in protection and security of homeland infrastructure will ensure immediate transition to the offense during a mass electrical outage.

The book *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* states:

> Any scenario between adversaries is a balance between offense and defense. When the offense has the advantage because of some combination of technological superiority or cost, military theorists write, there will be conflict. When the reverse is true, when it costs more to attack or when the chances of an attack defeating the defenses is low, greater stability will prevail.[16]

It is critical that the Marine Corps is proactive in defense (and transition to offense) of a cyber or electromagnetic attack or after a natural disaster. The Marine Corps has increased efforts to demonstrate resilient energy in support of some installations but development lags when considering the potential need.[17] Independence from domestic power sources demonstrate redundant installation security and energy efficiency and deter adversary threats. It is critical that the Marine Corps accelerate and prioritize installation energy resiliency in order to combat current cyber and electromagnetic threats and natural disasters—a solution is a unified task force assembled to thoroughly assess, test, and improve installation energy resiliency, while also enhancing network and operational resiliency. The alternative is electrical energy overreliance—a Marine Corps vulnerability.

Notes

1. Association of Defense Communities, *Beyond the Fence Line: Strengthening Military Capabilities Through Energy Resilience Partnerships*, (Washington, DC: 2018).

2. Ibid.

3. Business Executives for National Security, *Power the Fight: Capturing Smart Microgrid Potential for DoD Installation Energy Security*, (Washington, DC: 2012).

4. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018*, (Washington, DC: Office of the Secretary of Defense, 2018).

5. Ibid.