The Threat to the Electric Grid of Drones Must Be Analyzed and Action Taken Now

Steve Naumann, Chief Technical Advisor – Protect Our Power
snaumann@protectourpower.org

The recent attack on two North Carolina substations once again has highlighted the fact that the electric system remains a target for physical attack.[1] But intensifying Russian attacks on Ukraine's grid highlight another threat to US electric infrastructure – the potential use of armed Unmanned Aircraft Systems (UAS), commonly called drones, to strike substations and other critical assets.

Nation states and terrorists (foreign and domestic) have access to increasingly sophisticated UAS to conduct such attacks. Moreover, by attacking from above, adversaries can obviate the value of hardened fences and other physical defenses that BPS entities are currently deploying to comply with NERC Critical Infrastructure Protection (CIP) standards.

NERC is now reviewing the adequacy of these standards. As that effort goes forward, NERC and owners of Bulk Power System (BPS) facilities must take into account the risk of UAS attack. However, because of the work that needs to be done on the threat and effective defenses, I recommend in the analysis below that any requirements associated with the risks of UAS attacks must not be proscriptive. NERC, BPS entities, and the Department of Energy, and their partners, as well as state regulators, should also begin long-lead development of viable, cost-effective defense

[1] There have been subsequent physical attacks at four electric substations in the Tacoma, Washington area. U.S. Attorney's Office, Western District of Washington "Two charged with attacks on four Pierce County power substations," (Jan. 3, 2023), located at https://www.justice.gov/usao-wdwa/pr/two-charged-attacks-four-pierce-county-power-substations.

options. In particular, they should leverage the progress that National Laboratories and the Department of Defense are making in counter-UAS (C-UAS) technologies and systems.

Yet, the most difficult challenges to UAS defense lie in the realm of policy, not technology. Current statutory constraints, including criminal laws such as the Aircraft Sabotage Act, 18 U.S.C § 32, impose major limits on the ability of BPS owners/operators to defend substations and other assets against armed UAS, no matter how severe the risk those attacks pose to electric service, to Critical Defense Facilities and other vital customers.[2] Laws and regulations administered by the Federal Communications Commission prohibit, among other actions, the use of equipment "designed to block, jam, or interfere with wireless communications."[3] Other constraints on defense, such as complying with FAA laws and regulations concerning use of airspace, exist as well.[4] BPS entities should work with their partners to seek revisions for these policies, especially with regard to the use of jamming and other non-kinetic defenses to prevent adversaries from achieving their goals.

1. THE NATURE OF THE THREAT

The Russian campaign against Ukraine highlights key features of this threat, but also illuminates attacks against the US grid are likely to differ. For example, Russia has

[2] For a list of federal laws that may apply to detection and mitigation of threats from UAS, *see* DOJ/DOT/FCC/DHS Advisory on the Application of Federal Laws To The Acquisition and Use of Technologies to Detect and Mitigate Unmanned Aircraft Systems (Aug. 2020)(2020 Joint Advisory), located at https://www.cisa.gov/sites/default/files/publications/20_0817_ogc_interagency-legal-advisory-uas-detection-mitigation-technologies_1.pdf.

[3] *Id*. at unnumbered p.9. *See In the Matter of Ravi's Import Warehouse, Inc.*, FCC Rcd 22-10 (Jan. 27, 2022)(Statement of Chairwoman Rosenworcel, "When it comes to signal jammers, the Communications Act is clear. You can't make them, import them, sell them, ship them, or operate them.").

[4] 2020 Joint Advisory at unnumbered p.7.

a well-planned campaign to destroy the electric infrastructure of Ukraine.[5] Russia is able to do so by launching very large UAS (including the Shahed-136**)** from its own territory, and use its own infrastructure to maintain, launch and operate those drones for cross-border strikes

Potential US adversaries will lack comparable advantages of proximity to their own territories. But that proximity will not be necessary for striking US substations with smaller but well-armed drones. Much like the September 11 terrorists who used airplanes taking off from airports within the United States, the more likely threat is nation states or domestic violent extremists[6] using UAS at a scale, and launched from within the United States, to simultaneously attack multiple substations. Such an attack could be designed to cause significant destruction not only to the BPS, but also Defense Critical Electric Infrastructure and other critical distribution facilities, with devastating impacts that go far beyond what we have seen in North Carolina or at Metcalf.[7] In fact, given the potential for destroying substantial high-value equipment over a broad geographic area, physical attacks by UAS have the potential to cause more, a longer, disruptions to the electric system than do cyber attacks.

[5] The emphasis of this paper is to highlight the threat of UAS to the US electric grid. In order to fully understand the threat of UAS, it is important to note that Russia has accompanied its airborne attacks of Ukraine's energy sector with cyberattacks. Clint Watts, Preparing for a Russia cyber offensive against Ukraine this winter (Dec. 3, 2022), located at https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/.

[6] National Terrorism Advisory System Bulletin, Summary of the Terrorism Threat to the United States (Feb. 7, 2022), located at https://www.dhs.gov/sites/default/files/ntas/alerts/22_0207_ntas-bulletin.pdf.

[7] US Department of Defense, 2022 National Defense Strategy of the United States of America, at 5 ("The PRC or Russia could use a wide variety of tools to hinder U.S. military preparation and response in a conflict, including actions aimed at undermining the will of the U.S. public, and to target our critical infrastructure and other systems") (Oct. 27, 2022), located at https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

The threat to the homeland is very real. The FBI has warned owners of critical infrastructure that UAS may be used for surveillance of facilities[8] and potentially to deliver explosives.[9] In addition, UAS have been modified to damage electrical equipment, including through dragging conductive wires from a drone.[10] Even though Iranian-made military-grade UAS are being used by Russia in war in Ukraine, commercial UAS also are being used for reconnaissance and to drop munitions.[11] It does not take much imagination to see that sophisticated commercial UAS, especially those produced in China, can be a threat to the US electric grid.

II. DEFENSIVE OPTIONS

FERC already has directed NERC to review the physical security requirements for BPS facilities.[12] Some have suggested installing more effective barriers to protect equipment; increased surveillance; and patrolling by security personnel at all BPS substations is the solution. But fences or ballistic barriers to protect electric substations

[8] CNN, FBI Warns Drones Pose Potential Risk To Critical Infrastructure After Some Spotted Over Louisiana Chemical Facilities (Sept. 10, 2022), located at https://www.cnn.com/2022/09/30/politics/drones-risk-critical-infrastructure-spotted-louisiana-chemical-facilities/index.html.

[9] The Defense Post, FBI Probing Cases of Bomb-Laden drones in US (Nov. 18, 2022), located at https://www.thedefensepost.com/2022/11/18/fbi-bomb-laden-drones-us/; US Senate Committee on Homeland Security, Threats to the Homeland (Nov. 17, 2022)(video of hearing at 1:03:13 – 1:03:27), located at https://www.hsgac.senate.gov/hearings/11/16/2022/threats-to-the-homeland.

[10] Testimony of Samantha Vinograd before the Senate Committee on Homeland Security and Governmental Affairs at 3 (July 14, 2022)("drone . . . had been modified to cause an intentional power disruption"), located at https://www.hsgac.senate.gov/imo/media/doc/Testimony-Vinograd-2022-07-14-REVISED.pdf; CNN, Drone at Pennsylvania Electric Substation Was First to 'specifically target energy infrastructure,' According to Federal Law Enforcement Bulletin (Nov. 4, 2021), located at https://www.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation/index.html.

[11] Washington Post, Russia and Ukraine are Fighting the First Full-scale Drone War (Dec. 2, 2022), located at https://www.washingtonpost.com/world/2022/12/02/drones-russia-ukraine-air-war/; The Washington Institute for Near East Policy, What Iran's Drones in Ukraine Mean for the Future of War (Nov. 10, 2022),located at https://www.washingtoninstitute.org/policy-analysis/what-irans-drones-ukraine-mean-future-war.

[12] On December 15, 2022, FERC issued an order directing NERC to conduct a study (1) evaluating the adequacy of the criteria in the existing physical security standard, CIP-014-3; the required risk assessment; and whether a minimum level of physical security should be required at all Bulk Power System substations and control centers, and report to FERC within 120 days. *North American Electric Reliability Corporation*, 181 FERC ¶ 61,230 (2020)(Order Directing Report).

against high powered rifles are useless against threats from the air. Solutions also need to be able to protect equipment from aerial attack by UAS. Utilities and federal and state regulators will have to balance the risks to the continuity of electric service of kinetic attacks with the costs to customers, remembering that the electric system in the United States consists of over 70,000 transmission and distribution substations, many in rural areas and many easily accessible from roads and highways – and all accessible to the skies above them

It will take a great deal of study to explore hardening options, and some solutions may be so expensive as to be cost prohibitive. At the same time, infrastructure owners, policymakers and lawmakers need to consider the role of active defense systems (C-UAS capabilities), which likely will require federal legislation.

After the 2013 attack on the PG&E Metcalf Substation, FERC directed NERC to promulgate a physical security standard to protect the most critical Bulk Power System substations – those that "if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or cascading." The NERC Standard, CIP-014-3, requires among other things, for owners of these critical substations to evaluate "potential threats and vulnerabilities of a physical attack" and "develop and implement a documented physical security plan."[13] Although not required by the NERC Standard, utilities have also enhanced the security of other substations against physical attacks, generally prioritizing substations based on their importance.

While the requirement of CIP-014 to evaluate "potential threats and vulnerabilities" could include threats from UAS, the real question, given current legal

[13] NERC CIP-014-3 (2022).

and regulatory constraints,[14] is whether utilities and other owners of critical infrastructure presently can take *effective* measures to "deter, detect, delay, assess, communicate, and respond" to physical threats from UAS.

There are technologies to detect UAS in the vicinity of critical infrastructure that may not violate existing laws and regulations, and that allow infrastructure owners to detect, locate/track and classify/identify UAS. For example, using non-intrusive monitoring systems, utilities can gather data on UAS overflights and communicate that information to law enforcement authorities.[15] The more difficult question t is what actions can asset owners take to protect electric facilities against use of explosives or other kinetic attacks from the air, against adversaries who at present have air supremacy.

One possible solution would be to retrofit substations by enclosing some or all of the equipment. This solution poses engineering challenges first to decide whether to protect high value equipment or to protect entire substations. If the entire substation needs to be enclosed, there are engineering challenges to enclose existing substations to ensure equipment, such as transformers, are adequately cooled (a number of urban substations were designed to be fully enclosed in buildings). Moreover, fully enclosing substations is expensive and time consuming.

There presently are some technologies that appear promising at protecting high value equipment such as transformers such as The "Armored Transformer Barrier

[14] *See* 2020 Joint Advisory; Rupprecht, Big Problems with Counter Done Technology (Anti Drone Guns, Drone Jammers, Etc.), located at https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems/#Current_United_States_Counter_Drone_Law.

[15] *See, e.g.*, Dedrone, Customer Success Stories, https://www.dedrone.com/industry/critical-infrastructure.

System," developed by Idaho National Laboratory and licensed for manufacture.[16] Of note is that this product includes an optional "top-hat armor extension" which is critical to protect equipment from attacks by UAS. This type of technology may be a short-term solution while the engineering and threat analyses are being performed to determine whether to protect specific equipment or to enclose entire substations.

Given the number of substations in the US and the potential costs of fully enclosing substations, policymakers may need to start looking at active defenses, both non-kinetic (using electronic means such as jamming) and kinetic (which could include lasers and microwave as well as net guns).[17] The military is spending hundreds of millions of dollars and research, development and procurement of C-UAS technologies, including jamming and directed-energy weapons.[18]

III. POLICY AND STATUTORY CONSTRAINTS

As mentioned above, there are federal and state criminal laws that generally prohibit law enforcement and asset owners from implementing active defenses that interfere with or destroy UAS, regardless of the threat to critical infrastructure. This includes electronic means such as jamming and spoofing, as well as using kinetic means to bring down UAS. Moreover, the risk to the civilian population due to collateral damage as a result of active defenses against UAS would require careful study, on a

[16] Idaho National Laboratory, Armor Technology Designed To Protect The Power Grid Licensed By Michigan Company, located at https://inl.gov/article/armor-technology-designed-to-protect-the-power-grid-licensed-by-michigan-company/.

[17] *See* DHS, Counter-Unmanned Aircraft Systems Technology Guide, Section 3-4, pp. 22-24 & nn. vi and vii (Sept. 2019)(DHS C-UAS Technology Guide), located at https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf.

[18] Congressional Research Service, Department of Defense Counter-Unmanned Aircraft Systems (May 31, 2022), located at https://sgp.fas.org/crs/weapons/IF11426.pdf.

substation by substation basis, in order to decide what, if any defenses can be used and to approve rules of engagement.

A well-developed plan must include a review of present laws and recommend changes that will allow for protection of critical infrastructure, including active defenses. Both the Biden Administration[19] and more recently, Congress, have recognized the need to analyze and recommend changes to federal legislation to counter UAS threats.[20] Because the threat is here now, there is an expeditious need for legislation to ensure appropriate federal and state agencies, including local law enforcement, as well as owners of the electric grid, are able to take effective actions to protect critical infrastructure.

IV. LONGER-TERM SOLUTIONS THAT LEVERAGE THE GRID'S TRANSFORMATION

Another set of possible mitigation measures would be to increase the redundancy of the electric grid through additional substations that are geographically disbursed. This measure likely would be more effective for the bulk power system which is networked than for the distribution system, where there are more radial circuits and, because of lower voltages, substations need to be geographically closer to the load. Some emerging technologies also may help mitigate the threat. For example, the

[19] Fact Sheet: The Domestic Counter-Unmanned Aircraft Systems National Action Plan, Recommendation 1 (Apr. 25, 2022), located at https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/. The Domestic Counter-Unmanned Aircraft Systems National Action Plan, if adopted would include legislative proposals expand the entities that can protect against UAS, as well as "permit critical infrastructure owners and operators to purchase authorized equipment to be used by appropriate Federal or SLTT law enforcement agencies to protect their facilities."

[20] James M. Inhofe National Defense Authorization Act of Fiscal Year 2023, PL 117-263 (2023 NDAA), Section 162(b)(2)(E) (requiring DOD to analyze, determine and prioritize legislative action to ensure DOD has the ability to counter threats posed by UAS swarms).

use of superconducting cables can link distribution substations that are more geographically dispersed for faster restoration.[21] Finally, for some critical facilities, microgrids could provide resilience where substations feeding that area are damaged or destroyed.

The buildout of the electric grid to support integration of zero-carbon resources presents an opportunity to design resilience into the grid, both for the bulk power system and the local distribution system. With the expected expansion of zero-carbon distributed energy resources (DERs), distribution system planners can plan to network parts of the distribution system to be able to share distribution-level DERs to serve load during emergencies. Such a design would mitigate the impact of destruction of transmission and transmission-distribution substations by UAS.

Ultimately, utilities and other owners of critical infrastructure are being asked to protect those assets against terrorists, and in the extreme, nation states. At this point, mandatory NERC or state standards are at best, premature, and at worst could be counter-productive before there is an agreed upon Design Basis Threat (DBT) and an evaluation of protection methods against the UAS threat.

In the same way that the NRC developed a DBT in order to set requirements to protect nuclear power plants, a DBT for the UAS threat would need to look at the capabilities of adversaries to use UAS; the type of UAS and the capability to do damage; the number of UAS used in an attack; and the potential for assistance by insiders having knowledge of the grid. The DBT would be informed by lessons learned

[21] US Department of Energy, How Superconductors Are Helping Create the Resilient Grid of the Future (Dec. 1, 2021), located at https://www.energy.gov/oe/articles/how-superconductors-are-helping-create-resilient-grid-future. This technology, partially funded by the Department of Homeland Security, is in the demonstration stage.

from the use of UAS to attack the electric grid in Ukraine. Only then can owners of the electric grid facilities, regulators and policymakers start to determine the best and most cost-effective way to mitigate against the threat.

In contrast, Requirements 4-6 of CIP-014-3, requires the owners of the transmission facilities to evaluate potential threats and vulnerabilities; develop and implement a physical security plan; and have an unaffiliated third party review the evaluation and the proposed plan. For physical threats based on attacks from ground forces with capabilities that were well understood, this regime is appropriate. But for the developing threat of UAS, the industry needs a DBT and an understanding of defense options before it starts spending large sums of money that might not do the job.

V. RECOMMENDATIONS

The industry needs coordinated action by the US Government. The Department of Energy, the Sector Specific Agency for the energy sector, working with the Electricity Subsector Coordinating Council (ESCC) and critical infrastructure owners, should expeditiously review the UAS threat to the entire electric system, including the local distribution system, and based on a DBT and review of technologies, recommend passive and active defense measures against the UAS threat. DOE can work with its national laboratories, with other federal agencies with specific expertise, such as DOD, DHS, and the FBI, and with the owners of critical infrastructure, and therefore is best suited to recommend solutions for quick implementation. Because DOD is currently working on C-UAS technologies and has funding to test various methods for detecting and disabling UAS that threaten US forces and infrastructure, DOE should rely heavily

on this work to expedite protection of the grid, especially the most important substations, where kinetic protection may be necessary.[22]

DOE's focus should be on all elements of resilience:

- Best practices and technologies to legally detect and assess UAS activity near critical infrastructure[23]
- Best practices and technologies to protect critical infrastructure against UAS attacks
- Best practices and technologies to respond and recover from UAS attacks on critical infrastructure[24]
- A 'gap analysis' of existing practices informed by the DBT and actual events in Ukraine
- A review of the need for and the potential effectiveness of active defenses in civilian areas
- A review of federal and state laws that may prohibit protection of the electric grid by the US government, state and local law enforcement and asset owners and recommendation for changes to laws to effectively protect the electric grid against the UAS threat

We have seen Russia use UAS effectively to destroy major parts of the electric gird in Ukraine. Just like the Russian cyber attacks in 2015 and 2016 of Ukraine's electric grid, we have a preview of a threat for major destruction of portions of the US

[22] DOD must plan to acquire and obtain C-UAS swarms to defends its forces, other assets of the US and infrastructure. 2023 NDAA at Section 162(b)(2)(C).
[23] DHS C-UAS Technology Guide.
[24] Some technologies, such as modular portable transformers also will provide faster recovery from other threats such as GMD, EMP and physical attacks on the ground.

electric grid, not just from UAS physical attacks, but also combined with continual cyber attacks. The time to act is now, not after a UAS attack has already devastated multiple US substations and created blackouts far more severe and disruptive than those experienced in the North Carolina attacks.