Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

WHITE PAPER SERIES

Terrorist Targeting of U.S. Utilities Infrastructure

March 2022

INTENT

This white paper is designed to provide analysis of relevant, publicly available information on threat and hazard events/trends and their potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be an all-encompassing assessment of the subject.

Terrorist Targeting of U.S. Utilities Infrastructure

Introduction

In recent years, various terrorist groups and individuals (both transnational and domestic) have targeted utilities infrastructure in the U.S. with varying degrees of success. Utilities infrastructure (to include power, water, gas, and communications) remains an appealing target due to its fundamental role in sustaining the daily life and economic functions of society. Additionally, various portions of the U.S. utilities infrastructure often presents as a "soft target", without human security or substantial physical security in many cases. This paper will examine the terrorist targeting of U.S. utilities infrastructure as well as the various tactics, techniques, and procedures (TTPs) involved.

Background

Utilities generally fall within the broader scope of critical infrastructure. The U.S. federal government divides critical infrastructure into 16 distinct sectors. Critical infrastructure sectors are defined as those "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[1] This includes both physical and virtual systems and networks. The 16 U.S.-defined critical infrastructure sectors includes sectors such as commercial facilities and financial services (which may be also targeted by terrorists). However, utilities (to include power, water, gas, and communications) form a backbone supporting the daily functionality of societies around the globe, and as such will be the primary focus of this paper.[2]

Broadly speaking, terrorists aim to use force, violence, or threats against persons or property with the aim to coerce a state or people based on a political or social ideology. Generally, attacks are premeditated and committed against noncombatant targets.[3] Utilities infrastructure remains a highly appealing target. A successful attack on utilities infrastructure, whether physical or virtual, could trigger fear and economic losses, as well as present a threat to the health and safety of the public. Furthermore, the interdependencies of critical infrastructure mean that the failure of one sector can lead to a diminishing or complete failure of one or more other sectors. A successful attack on a single utility may have cascading effects, furthering the impact and disruption sought by the attacker.[4] Additionally, critical infrastructure failures disproportionately affect socially vulnerable populations.[2]

While some utilities have been hardened against threat actors, the sheer size and scope of utilities in the United States leads to many physical utility locations remaining "soft targets." Soft targets are those that are easy to attack, unprotected, and vulnerable. Generally, they are also publicly accessible. Though utilities infrastructure would generally lack the symbolic appeal of some targets, the ease of access increases appeal to threat actors.[5] Furthermore, most critical infrastructure in the United States is owned and operated by the private sector. Public-private sector partnerships are key in ensuring utilities are secured. A successful attack on utilities could lead to the degradation or failure of essential public functions and requirements.

Transnational Terrorists

Transnational terrorist organizations have shown historically that they are capable and willing to target utilities infrastructure in furtherance of their ideological objectives. According to the START Global Terrorism Database, there have been at least 212 instances of utilities infrastructure being the target of terrorist attacks worldwide as of 2018-2019 (the most recent year available).[6] As early as 2002, there were clear indications that al-Qaeda (AQ) was seeking to exploit vulnerabilities in U.S. public and private utilities. The energy sector has witnessed sustained transnational terrorist activity through attacks perpetrated by AQ and the Islamic State (IS). Key water infrastructures have been the object of particular attention on the part of IS. Between 2013 and 2015, IS launched around 20 major attacks against Syrian and Iraqi targets. In addition to destroying pipes, sanitation plants and bridges, IS has used water infrastructures strategically, for example by closing dams and cutting off water supplies.[11]

Nuclear plants, another key asset in the utilities infrastructure realm, have a demonstrated history of being targeted by transnational terrorists. One (1) case in 2021 saw 15 rockets directed and fired towards the Negev Nuclear Research Facility in Israel by Hamas militants. Though the facility is research-focused, this direct, physical attack on a nuclear facility illustrates a clear intent to target associated infrastructure.[7] Throughout this Israel-Palestine conflict in 2021, Hamas sought to target other areas of Israeli critical infrastructure and utilities such as oil facilities and pipelines. As hundreds of rockets were launched by Hamas, at least one (1) rocket made direct contact with a Trans-Israel pipeline and oil reserve running from the Mediterranean to the Red Sea.[8,9] Utilities infrastructure such as oil pipelines, reserves, and facilities are deemed critical infrastructure by states worldwide and Hamas took advantage of this by directing its efforts to destabilize these Israeli utilities infrastructure.

The Islamic Revolutionary Guard Corps (which, despite Iranian government affiliations, is a recently recognized foreign terrorist organization) attempted to target U.S. utilities infrastructure in the form of a small dam 25 miles north of New York City. Hackers broke into the command-and-control system of the dam in 2013, apparently through a cellular modem. Should this mission have succeeded, the hackers would have been able to release water from behind the dam with remote access and potentially threaten public health and safety. Although this mission failed, the incident signaled the desire of some transnational terrorist organizations to infect, and potentially operate, U.S. infrastructure via cyberattacks.[10, 11]

Acts of transnational terrorism, as seen above, have involved events in countries across the globe including the United States. Similar acts of direct, indirect, and exploitation TTPs may be used to target utilities infrastructure in the United States such as communications, energy, water/wastewater, and nuclear systems/infrastructure. The use of more physical, direct methods of attack on utilities infrastructure (to include the use of Unmanned Aerial Systems, or UAS) and indirect or remote usage of cyber technology to exploit, hack, and disrupt utilities infrastructure are also becoming increasingly likely TTPs. However, transnational terrorist organizations may not need to coordinate attacks from overseas. Attacks on utilities infrastructure in the United States can also come from self-radicalized "lone wolves" or small groups of individuals who affiliate themselves with extremist ideologies of certain transnational terrorist organizations. Many larger transnational terrorist organizations such as IS and AQ publish propaganda online to help generate

cells in other countries abroad.[12] These lone wolves or small self-radicalized cells may target U.S. utilities infrastructure as an act of support to various transnational terrorist organizations and their ideologies.

Domestic Terrorists/HVEs

A January 2022 bulletin from the Department of Homeland Security (DHS) was quoted in open sources, stating that domestic violent extremists (DVEs) have developed "credible, specific plans" to attack utilities infrastructure in the U.S. since at least 2020.[13] However, notable attacks on utilities infrastructure by DVEs occurred prior to 2020. In April 2013, one or more unknown perpetrators attacked an electrical substation in Metcalf, California and cut fiber-optic phone lines to disconnect service to nearby neighborhoods. The attackers also fired more than 100 rounds of .30-caliber rifle ammunition at 17 electricity transformers, causing $15 million in damages.[14] In June 2019, unknown suspects fired shots at a transformer and power regulators located at a substation in Klamath Falls, Oregon. Approximately 1,000 customers lost power and the damage totaled more than $400,000.[15] Power stations, water treatment plants, and telecommunications sites are often both publicly visible and accessible, making them more attractive targets for DVEs. Fencing and traditional security measures can sometimes be circumvented. In one instance, a UAS of unknown origin was flown into an electrical substation in Pennsylvania in 2020. The drone crashed without causing damage. It was modified with a trailing tether supporting a length of copper wire, which could have caused a short-circuit if it touched high-voltage equipment.[16] Attacks can also come from cyberspace. In February 2021, a hacker remotely accessed a water treatment plant in Oldsmar, Florida and increased the levels of sodium hydroxide in the water. A supervisor noticed the change and reversed it before any damage could occur. However, the water would have been poisonous had the mixture reached customers. The identity and location of the hacker are still unknown, but the incident demonstrates the vulnerability of utilities infrastructure to a cyberattack.[17]

Some of the plotting against utilities infrastructure amounts to little more than discussion and encouragement on social media and secure messaging platforms.[18] Other instances are planned and organized over months by well-established DVE groups, including the National Socialist Order (NSO; formerly Atomwaffen Division). The NSO is an accelerationist neo-Nazi group that began in 2015 in the U.S. but has affiliates overseas. The group's cells are decentralized to mitigate counterterrorism efforts by law enforcement. Adherents of the group have been arrested for targeting utilities infrastructure at least twice, along with other violent crimes.[19] In 2017, the group's founder was arrested in conjunction with a murder plot among other members. In January 2018, he was sentenced to five years in prison for possessing explosive material intended for use against nuclear facilities.[19] In August 2021, four members of NSO, including two former U.S. Marines, were charged with conspiracy to damage the property of an energy facility. The group conspired to detonate homemade explosive devices at transformers, substations, or other component of the electrical grid in Idaho and the Northwestern U.S. Their trial is pending.[20]

DVE attacks on utilities infrastructure can also come from self-radicalized "lone wolves" or small groups of individuals who affiliate themselves with extremist ideologies. From April 2020 to May 30, 2020, three members of the "Boogaloo Bois" movement conspired to use fire and explosives to attack government buildings and a Las Vegas electrical substation. Two of the men were

veterans in the Air Force and Navy, respectively, and one was an Army Reservist. They were indicted in June 2020 and are still awaiting trial. The Boogaloo movement lacks structure and leadership. Its name is derived from the 1984 film *Breakin' 2: Electric Boogaloo* to denote an unnecessary sequel. In this case, it refers to the group's believe in the inevitability of a Second American Civil War. Some adherents of the Boogaloo movement espouse white supremacist beliefs. Others are generally anti-authority and have even made common cause with left-wing groups during periods of civil unrest.[21,22,23]

In February 2022, three self-stylized neo-Nazis pleaded guilty to planning to attack power grids in the U.S. in the name of white supremacy. Each defendant was assigned a different substation to assault with a high-powered rifle. They believed the subsequent disruption, power loss, and economic impact would foment unrest and an eventual race war. They reportedly read and praised the same or similar foundational neo-Nazi texts as the NSO.[24,25] In both this case and that of the Boogaloo adherents, the attackers targeted utilities infrastructure after being radicalized online without joining an established DVE group.

Homegrown Violent Extremists (HVEs) also pose an ongoing threat to utilities infrastructure. Unlike their domestic counterparts, HVEs are typically inspired by Foreign Terrorist Organizations (FTOs). They often self-radicalize online and then act alone. Both ISIS, al-Qaeda, and their affiliates have encouraged followers abroad to carry out attacks on their own. There have been attacks within CONUS by HVEs meeting these criteria. Usually, these HVEs have attacked soft targets, including pedestrians using a truck and, in one case, an attempted suicide bombing in a bus terminal. However, there is a dearth of reported incidents in which HVEs inspired by FTOs targeted utilities critical infrastructure withing CONUS in the past 20 years.

Outlook

Both foreign and domestic terrorist groups and individuals will almost certainly continue to target U.S. utilities infrastructure due to a variety of factors, to include the "soft target" posture of various utilities nodes, as well as the devastating impacts to public health and safety and the economy that infrastructure disruptions can cause. Moreover, emerging TTPs such as cyberattacks and the use of UAS remain a concern. RMC's Intelligence & Analysis Division continues to monitor trends related to terrorist targets, as well as the various TTPs utilized by terrorists.

---

[1] Critical Infrastructure Sectors. (n.d.). CISA. Retrieved March 2, 2022, from https://www.cisa.gov/critical-infrastructure-sectors

[2] Sandholz, S. (2017, October 5). Five things you need to know about critical infrastructures. Institute for Environment and Human Security. Retrieved March 2, 2022, from https://ehs.unu.edu/blog/5-facts/5-things-about-critical-infrastructures.html

[3] C., C. (2014, April 8). Definition of Terrorism. SecBrief.Org. Retrieved March 2, 2022, from https://www.secbrief.org/2014/04/definition-of-terrorism/

[4] What Is Critical Infrastructure? Why Does Critical Infrastructure Security Matter? (n.d.). Palo Alto Networks. Retrieved March 2, 2022, from https://www.paloaltonetworks.com/cyberpedia/what-is-critical-infrastructure

[5] Martin, R. H. (2016). Soft targets are easy terror targets: increased frequency of attacks, practical preparation, and prevention. Forensic Research & Criminology International Journal. Retrieved March 2, 2022, from https://medcraveonline.com/FRCIJ/FRCIJ-03-00087.pdf

[6] START Global Terrorism Database. (2020 July). Global Terrorism Overview: Terrorism in 2019. Retrieved March 2, 2022, from https://www.start.umd.edu/pubs/START_GTD_GlobalTerrorismOverview2019_July2020.pdf.

[7] START. (n.d.). Nuclear Facilities Attack Database. Retrieved March 2, 2022, from https://www.start.umd.edu/nuclear-facilities-attack-database-nufad.

[8] O'Connor, T. (2021, May 12). Hamas Targets Israel Nuclear Site, Oil Line to Arab World as Conflict Death Toll Rises. Retrieved March 2, 2022, from https://www.newsweek.com/hamas-targets-israel-nuclear-site-oil-line-arab-world-conflict-death-toll-rises-1590880.

[9] ZeroHedge. (2021, May 14). Hamas Targets Israeli Oil and Nuclear Facilities with Rocket Attacks. Retrieved March 2, 2022, from https://oilprice.com/Geopolitics/Middle-East/Hamas-Targets-Israeli-Oil-And-Nuclear-Facilities-With-Rocket-Attacks.html.

[10] U.S. Department of State. (2019, April 8). Designation of the Islamic Revolutionary Guard Corps. Retrieved March 2, 2022, from https://2017-2021.state.gov/designation-of-the-islamic-revolutionary-guard-corps/index.html.

[11] CTED & UNOCT. (2018). The Protection of Critical Infrastructures Against Terrorist Attacks: Compendium of Good Practices. Retrieved March 2, 2022, from https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf.

[12] Tsesis, A. (2017). Social Media Accountability for Terrorist Propaganda. Retrieved March 2, 2022, from https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5444&context=flr.

[13] Sullivan, J. (2022, January 25). DHS Warns That Right-Wing Extremists Could Attack Power Grid. Retrieved March 1, 2022, from https://www.thedailybeast.com/dhs-warns-that-right-wing-extremists-could-attack-power-grid?source=articles&via=rss.

[14] Pagliery, J. (2015, October 17). Sniper Attack on California Power Grid May Have Been 'An Insider,' DHS Says. Retrieved March 1, 2022, from https://money.cnn.com/2015/10/16/ technology/sniper-power-grid/.

[15] FBI Portland. (2020, February 21). FBI Seeking Information in Klamath Electrical Substation Shooting. Retrieved March 1, 2022, from https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-seeking-information-in-klamath-electrical-substation-shooting.

[16] Hambling, D. (2021, November 5). Drone Used in Attack on US Electrical Grid Last Year, Report Reveals. Retrieved March 1, 2022, from https://www.newscientist.com/article/2296480-drone-used-in-attack-on-us-electrical-grid-last-year-report-reveals/.

[17] Chappell, B. (2021, February 9). FBI Called In After Hacker Tries To Poison Tampa-Area City's Water With Lye. Retrieved March 1, 2022, from https://www.npr.org/2021/02/09/965791252/fbi-called-in-after-hacker-tries-to-poison-tampa-area-citys-water-with-lye.

[18] Hanrahan, J., Thompson, A.C., & Winston, A. (2018, February 23). Inside Atomwaffen As It Celebrates a Member for Allegedly Killing a Gay Jewish College Student. Retrieved March 1, 2022, from https://www.propublica.org/article/atomwaffen-division-inside-white-hate-group.

[19] Stanford Center for International Security and Cooperation. (2021). Atomwaffen Division/National Socialist Order. Retrieved March 1, 2022, from https://cisac.fsi.stanford.edu/mappingmilitants/profiles/atomwaffen-division#text_block_23258.

[20] Dept. of Justice. (2021, August 20). Group With Ties to Racially Motivated Violent Extremists Including Two Former Marines Facing Additional Charge of Targeting Energy Facilities. Retrieved March 1, 2022, from https://www.justice.gov/usao-ednc/pr/group-ties-racially-motivated-violent-extremists-including-two-former-marines-facing.

[21] Dept. of Justice. (2020, June 17). Federal Grand Jury Indicts Three Men For Seeking To Exploit Protests In Las Vegas And Incite Violence. Retrieved March 1, 2022, from https://www.justice.gov/usao-nv/pr/federal-grand-jury-indicts-three-men-seeking-exploit-protests-las-vegas-and-incite.

[22] Komenda, E. (2020, June 4). Men Tied to 'Boogaloo' Movement Conspired to Spark Protest Violence in Las Vegas, Feds Say. Retrieved March 1, 2022, from https://www.usatoday.com/story/news/nation/2020/06/04/boogaloo-movement-terrorism-related-charges-3-men-feds-say/3147563001/.

[23] Thompson, J. (2021, June 30). Examining Extremism: The Boogaloo Movement. Retrieved March 1, 2022, from https://www.csis.org/blogs/examining-extremism/examining-extremism-boogaloo-movement.

[24] Dept. of Justice. (2022, February 23). Three Men Plead Guilty to Conspiring to Provide Material Support to a Plot to Attack Power Grids in the United States. Retrieved March 1, 2022, from https://www.justice.gov/opa/pr/three-men-plead-guilty-conspiring-provide-material-support-plot-attack-power-grids-united.

[25] Zuckerman, J. (2022, February 24). Ohio Man Pleads Guilty to Plotting a White Supremacist Attack on Power Grid. Retrieved March 1, 2022, from https://www.citybeat.com/news/ohio-man-pleads-guilty-to-plotting-a-white-supremacist-attack-on-power-grid-12710668.