POLICY REPORT

Domestic Violent Extremist Targeting of the U.S. Electrical Transmission Grid

NEW LINES INSTITUTE
FOR STRATEGY AND POLICY

NOVEMBER 2023

Domestic Violent Extremist Targeting of the U.S. Electrical Transmission Grid

By Daryl Johnson and Alejandro J. Beutel

Contents

Executive Summary 3
Policy Recommendations 4
Introduction 4
Defining Scope, Key Terms, and Concepts 5
"Power Grid," "Transmission Grid," and "Critical Infrastructure" 5
Violent Extremist Vulnerabilities of the Transmission Grid 5
Domestic Violent Extremists (DVEs) 6
Background 6
A Brief History of Domestic Violent Extremist Attacks Against the Transmission Grid 6
U.S. Government and Industry Security Measures 7
Violent Far-Right Extremist Targeting of the Electrical Sector 10
Threat Assessment Overview 10
White Supremacists 11
Militia Extremists 12
Violent Far-Left Extremist Targeting of the Electrical Sector 12
Threat Assessment Overview 12
Violent Ecological Extremists 14
Left-Wing Anarchist Extremists 15
Other 15
Policy Recommendations 16
Ongoing Challenges 17
Endnotes 18

The content and views expressed in this intelligence briefing are those of the authors and should not be taken to reflect an official policy or position of the New Lines Institute for Strategy and Policy.

COVER: Photo illustration of the U.S. at night with city lights illuminated. (da-kuk / Getty Images)

The New Lines Institute for Strategy and Policy

Our mission is to provoke principled and transformative leadership based on peace and security, global communities, character, stewardship, and development.

Our purpose is to shape U.S. foreign policy based on a deep understanding of regional geopolitics and the value systems of those regions.

Executive Summary

Although threats against infrastructure are hardly a new issue, recent warnings about a resurgence of terrorist threats to the U.S. power grids have come from members of the U.S. Congress, government agencies like the U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI), and academic researchers. Ranking high among the various threats to the U.S. power grid is the threat of physical attacks by violent extremists. Both far-left and far-right domestic violent extremists (DVEs) pose threats to the transmission and distribution components of the U.S. power grid (hereafter "transmission grid").

The transmission grid has three main vulnerabilities that violent extremists may seek to exploit:

1. **Physical:** damage to exposed equipment and infrastructure.
2. **Cyber:** machine failures induced through computer-based disruptions, such as malicious software and denial-of-service attacks.
3. **Personnel:** including both direct physical attacks on transmission grid workers, as well as attempts to establish malicious insiders within the workforce through recruitment/radicalization and infiltration.

Of the three attack options, DVEs such as violent white supremacists, violent militia extremists, and violent eco-extremists are most likely to favor physical attacks. This is due to their familiarity with the technical capabilities and other operational tradecraft necessary to plan and execute physical attacks as well as ideological beliefs that inform attack strategy and operational behaviors. Although physical attacks are likely to be directly executed by people, there are signs that DVEs are engaging in operational innovations and could eventually incorporate aerial drones into attack planning and execution.

The authors' research – based on chat groups,[1] ideology, and conspiracy theories, as well as

Workers repair damage following an attack on two Duke Electric power substations in Carthage, N.C. The attack left tens of thousands without power in Moore County on Dec. 05, 2022. (Peter Zay / Anadolu Agency via Getty Images)

narratives that inform targeting preferences,[2] recent terrorist plotting arrests, and attack capability – indicates that violent far-right extremists are the most likely DVEs to physically attack the transmission grid and cause the most damage. The two submovements demonstrating the greatest intent and capacity to carry out physical attacks against the transmission grid are white supremacists and militia extremists. In addition to an ideologically motivated openness toward generating casualties, their well-established record of extensive possession of and training with caches of firearms, incendiaries, and explosives means that violent far-right attacks will likely continue to manifest in the form of shootings, arsons, and bombings.

Compared to violent far-right extremists, far-left extremists pose a much lesser (but nontrivial) potential threat of physical attacks against the transmission grid. The violent far-left extremists most likely to target the transmission grid are violent eco-extremists, violent left-wing anarchist extremists, and violent far leftists primarily motivated by social causes, such as anti-war and

anti-racist movements. While there is currently a lull in attacks specifically against the electrical sector, violent far-left actors continue to merit attention because, to the extent they pose a violent threat, they have targeted other aspects of the wider U.S. energy sector (e.g., attacks against pipeline projects), which could expand into resumed targeting of the transmission grid. Any future physical attacks against the transmission grid are most likely to manifest in arson attacks and so-called monkey wrenching – acts of sabotage such as cutting wires or removing screws, nuts, and bolts from support structures. Far leftists have technical familiarity with these attack methods, and they tend to favor acts of sabotage directed at property rather than people due to an ideologically motivated aversion to generating casualties.

Although violent far-left and violent far-right actors are not known to have committed cyberattacks against the power grid, including its transmission and distribution components, this may become an increasingly attractive attack option over time, especially in simultaneous use with physical attacks. This is due in part to actors' active online presence, as well as the growing availability of Malware-as-a-Service and Infrastructure-as-a-Service offerings in illicit/illegal cybermarkets that effectively outsource and rapidly scale up capabilities at minimal cost to the buyer. The potential impact of this threat is compounded by the growing use of artificial intelligence and machine learning methods among malware creators and cyberattackers.

Finally, insofar as threats to personnel are concerned, there is no evidence to currently suggest transmission grid workers are targeted for violence by violent extremists (either far-right or far-left). Currently, there are also no known cases of extremist insider threats within the transmission grid sector. However, given the lack of data on insider threat cases and the known nontrivial presence of extremists (particularly violent far rightists) in other parts of the wider energy sector, this possibility cannot be easily dismissed.

Policy Recommendations

To guard against and mitigate potential DVE threats and attacks against the U.S. electrical sector, policymakers in government should consider these recommendations:

- Update practices related to insider threats.
- Improve planning for future threats.
- Expand data-driven approaches to risk assessment and resource allocation.
- Support further research on violent extremist targeting of critical infrastructure, including electrical sector assets and personnel.

Introduction

Often called the "world's largest machine,"[3] the U.S. electric grid is one of humanity's most impressive engineering accomplishments. However, it is also aging and highly vulnerable to numerous human-made and natural disasters, ranging from accidents at power stations to extreme weather events like the 2021 severe winter storms that led to the statewide electric infrastructure failure in Texas.[4]

(Justin Sullivan / Getty Images)

Interrupted service can disrupt daily routines, impose severe economic costs that impact livelihoods, and effectively threaten lives by cutting off access to emergency services and residential heating/cooling during severe temperature events.

Ranking high among the various threats to the U.S. power grid is the threat of physical attacks by violent extremists motivated by various ideologies. The threat is not a new issue; members of the U.S. Congress,[5] government agencies like the U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI),[6] and academic researchers[7] have warned about resurgent terrorist threats to critical infrastructure, including the power grid.

Defining Scope, Key Terms, and Concepts

"Power Grid," "Transmission Grid," and "Critical Infrastructure"

In its most basic form, any electric power grid is composed of three parts: electricity generation, transmission, and distribution. What is often referred to as the U.S. electric grid (hereafter "the power grid") is an enormous web of power stations, transmission lines, and distribution entities spanning across the entire lower 48 states of the continental United States, the majority of where Canada's population lives, and the far northern part of Baja California, Mexico, that encompasses major cities such as Tijuana and Mexicali.[8]

The U.S. power *transmission* grid (hereafter "transmission grid") is the focus of this brief. The transmission grid refers to the transmission and distribution components of the wider U.S. power grid and includes millions of miles of high- and low-voltage power lines, as well as approximately 55,000 to 65,000 transformer substations.[9] The transmission grid is vulnerable to attacks by violent extremists. By comparison, power stations generating electricity are generally better defended, and violent extremists historically have attacked and plotted against them less often.[10]

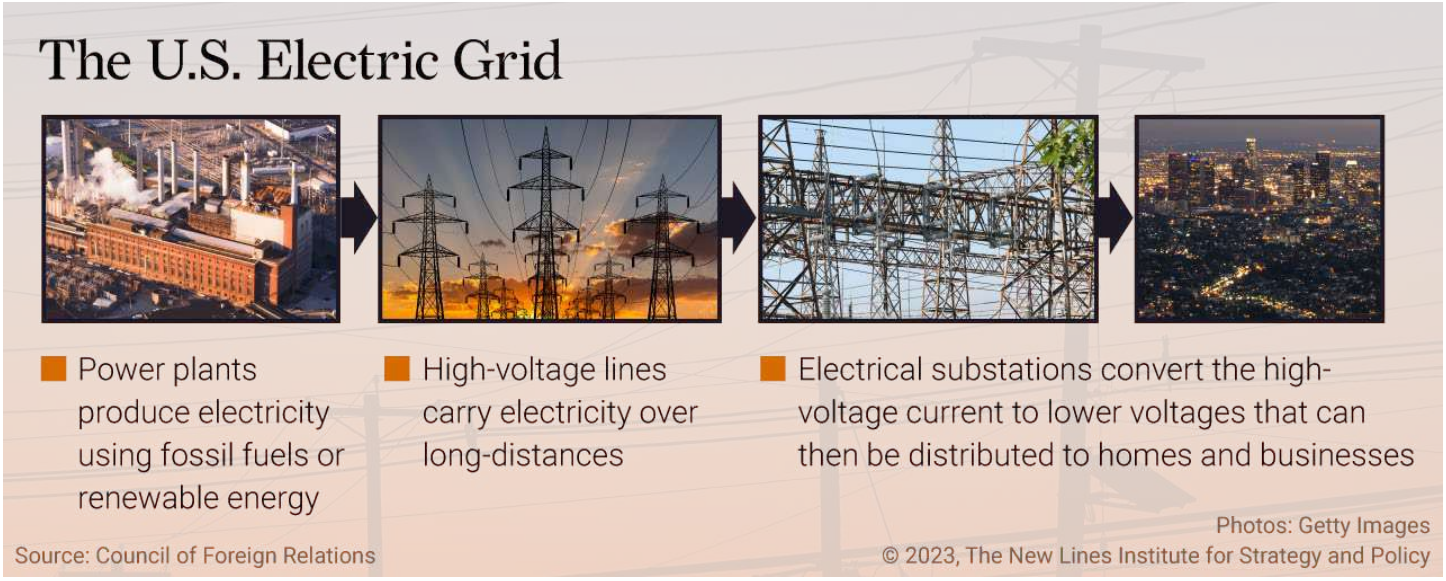
The transmission grid collectively falls within what federal legislation calls "critical infrastructure," a term used to describe "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[11]

Violent Extremist Vulnerabilities of the Transmission Grid

A study published in 2012[12] by the U.S. government-funded National Research Council, "Terrorism and the Electric Power Delivery System," identifies three types of vulnerabilities that violent extremists can exploit to attack the transmission grid:

1. **Physical:** damage to exposed equipment and infrastructure.
2. **Cyber:** machine failures induced through computer-based disruptions, such as malicious software and denial-of-service attacks.
3. **Personnel:** including both direct physical attacks on transmission grid workers, as well as attempts to establish malicious insiders within the workforce through recruitment and infiltration.

Violent extremists exploiting physical vulnerabilities of the transmission grid were the most prevalent threat manifestation in the past and appear to be the most likely means of attack in the present and near future. However, the authors will also discuss cyber and personnel vulnerabilities insofar as how they potentially intersect with and/or coexist as potential attack options alongside physical assaults on transmission grid infrastructure.



Domestic Violent Extremists (DVEs)

The authors have adopted the U.S. intelligence community's definition of a DVE, which is an actor "based and operating primarily in the United States without direction or inspiration from a foreign terrorist group or other foreign power and who seeks to further political or social goals wholly or in part through unlawful acts of force or violence."[13] This definition is largely focused on analyzing government actions and is tailored to audiences interested in federal-level policy. Furthermore, this definition is based on a comprehensive threat assessment that was produced in consultation with government departments and agencies that typically have led efforts to combat terrorism and violent extremism within U.S. borders, including the Department of Justice and the DHS. Therefore, the authors interpret this as a U.S. government-wide "consensus" definition, or at least a reasonably close approximation of one.

In addition to their potential physical threats to the transmission grids, with the exception of violent white supremacist/white nationalist extremists, the other listed ideological submovements have been underexplored in recent relevant studies on violent extremist threats to critical infrastructure.[14] The authors' focus on DVEs means nonstate actors considered in U.S. government policies as "foreign-inspired" (e.g., nonstate transnational terrorists, and "homegrown" violent extremists[15] aligned with al Qaeda, the Islamic State, or al Shaabab, among others) are outside the scope of this publication.

Key Far-Right and Far-Left Groups

Based on recent past and/or present attempts to physically attack the U.S. power grid, the authors have focused on these subsets of DVEs:

Far Right

- **Violent white supremacist/white nationalist extremists:** These are actors who believe "white" people are genetically, morally, and/or culturally superior to all other races. They also tend to be overwhelmingly antisemitic, anti-immigrant, and express intense hatred toward sexual and gender minorities as well as individuals they deem as "parasites" upon society, such as people without housing.
- **Violent militia extremists:** A subset of the wider far-right antigovernment extremist movement, they are primarily mobilized by intense fear and loathing of government actors – especially those representing the federal government. They tend to emphasize paramilitary training and organizational structure in reaction to what they see as government threats to citizens' constitutional rights.

Far Left

- **Violent eco-extremists:** These are actors motivated by the intent to reduce or end harm and destruction of the environment (both perceived and real), including all parts of the ecosystem.
- **Violent left-wing anarchist extremists:** These are actors who "oppose all forms of capitalism, corporate globalization, and governing institutions, which are perceived as harmful to society."
- **Other:** These are individuals adhere to left-wing ideologies but are not primarily motivated by anarchist beliefs or ecological concerns. This category includes Black nationalists and anti-pro-life extremists.

Sources: Office of the Director of National Intelligence, author definitions

Background

A Brief History of Domestic Violent Extremist Attacks Against the Transmission Grid

A 2016 study from the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland found violent extremists conducted over 2,000 attacks against all three elements of the U.S. power grid between 1970 and 2015. Most of those attacks, however, were directed at its transmission and distribution components and conducted by actors who would be classified under current federal policy as DVEs. DVE targeting

of the transmission grid using small-scale attacks against electrical sector targets (primarily electric substations, transformers, and high-voltage transmission lines) has continued over the past decade.[16]

So far, these attacks and aspirational terrorist plots have had limited impact in terms of directly disrupting service. The extremists' goals, however, are to cause local or widespread blackouts and disrupt the daily operation of society. For far-right violent extremists, these attacks are often directly connected to wider operational plans toward a desired strategic end goal of overthrowing our current system of government. For far-left violent extremists, such as eco-extremists, the goal is often much narrower, such as drawing attention to a particular issue (i.e., reliance on fossil fuels, climate change, corporate greed, or generating pollution).

Several vandalism and sabotage incidents against electrical substations and transformers remain unsolved; thus, perpetrators' motives remain unknown, but the possibility of connections to DVEs remains open.[17] For example, on April 16, 2013, snipers shot more than 100 high-powered rifle rounds at several electrical transformers at the Metcalf substation near San Jose, California.[18] The perpetrators then scaled down into an underground vault and cut phone cables, which took out phone service, including 911 communications, in the surrounding area.[19] The case remains unsolved to this day but served as a watershed moment for the physical security of transmission grid assets. There have been no claims of responsibility related to these criminal acts, unlike in past years.[20] Nevertheless, this attack, among others, used tradecraft similar to other vandalism and sabotage incidents directly attributed to past DVE plots and physical attacks against U.S. critical infrastructure in general.

U.S. Government and Industry Security Measures

Federal policies seeking to secure the transmission grid from violent extremist attacks start with defining "critical infrastructure." This definition and similar articulations of it in other federal policy publications establish the foundation for the current U.S. government-wide strategy to protect critical infrastructure, the 2013 National Infrastructure Protection Plan (NIPP 2013). NIPP 2013 – an evolution of other NIPPs published in 2006 and 2009 – among other things categorizes critical infrastructure into 16 unique sectors, including the energy sector, which includes transmission grid security. While the DHS's Cybersecurity and Infrastructure Security Agency (CISA) is the federal entity in charge of coordinating all critical infrastructure security and resilience efforts, under NIPP 2013 the Department of Energy (DOE) is the lead agency for the energy sector[21] and developed a sector-specific plan in 2015 in conjunction with DHS.[22] On Dec. 17, 2020, CISA published four NIPP Supplemental Tool publications intended as "resources that can be used for members of the critical infrastructure community as they implement specific aspects of the plan."[23]

In addition to interdepartmental coordination and action, the federal government also regularly engages nongovernmental actors responsible for the daily operation and maintenance of the transmission grid. At the national policy level, this is largely mediated through the relationship between the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC). FERC, which is organizationally housed under the DOE – but is an independent agency (i.e., has regulatory authorities largely insulated from presidential and congressional control) – sets baseline security requirements and oversees the implementation of those standards by NERC. NERC, an international nonprofit entity composed of American and Canadian public utilities, is the federally designated U.S. electric reliability organization that articulates and promulgates more detailed versions of FERC-established baseline standards to its constituent public utility companies.[24]

Prior to the April 2013 Metcalf attack, post-9/11 critical infrastructure protection efforts mainly focused on the cybersecurity realm, despite numerous physical attacks attributed to violent extremists. However, after the Metcalf attack, more policy attention went toward increasing focus on the physical security of transmission grid infrastructure and personnel.[25]

Timeline of U.S. Federal Policy to Protect the Transmission Grid

1968: The National Electric Reliability Council, a voluntary trade association of U.S. based utility operators, is established.

1981: The National Electric Reliability Council, became the North American Electric Reliability Council, reflecting the participation of Canadian operators and stakeholders.

1998: President Bill Clinton signs Presidential Decision Directive (PDD) 63. Focused on critical infrastructure protection, among other things, the PDD is notable for defining "critical infrastructure," making critical infrastructure protection against physical and cyber threats a key federal policy priority, establishing lead agencies in charge of protecting specific sectors, establishing public-private partnerships as the general framework for advancing critical infrastructure protection, and calls for the establishment Information and Analysis Sharing Centers (ISACs).

2000: In response to PDD 63, the North American Electric Reliability Council establishes its sector-specific ISAC, the Electricity Sector Information Sharing and Analysis Center.

2001: U.S. Congress passes the USA Patriot Act one month after the September 11, 2001 terrorist attacks. The law includes a provision that statutorily defines "critical infrastructure."

2003: PDD 63 and relevant provisions in the USA Patriot Act are expanded upon and updated under the George W. Bush administration when it promulgated Homeland Security Presidential Directive (HSPD) 7.

2005: U.S. Congress passes the Energy Policy Act of 2005. Among other things, the law calls for the establishment of an Electric Reliability Organization (ERO), certified by Federal Energy Regulatory Commission (FERC) to "establish and enforce reliability standards for the bulk-power system, subject to Commission review."

2006: The George W. Bush administration publishes the first National Infrastructure Protection Plan (NIPP). North American Electric Reliability Council became the North American Electric Reliability Corporation (NERC). In addition to the name change, it was granted ERO status from FERC.

2007: DHS established National Protection and Programs Directorate (NPPD). Included within NPPD was the Office of Infrastructure Protection.

Transmission lines and towers sit behind barbed wire near the Energy Research Park in Houston, Texas. (Brandon Bell/Getty Images)

2009: The Barack Obama administration publishes the second NIPP.

2013: In February the Barack Obama administration issues Presidential Policy Directive (PPD) 21. The PPD's three overarching goals were to clarify relationships across the federal government to enhance critical infrastructure protection, enable better information sharing between public and private sector actors, and inform planning and operations through enhanced integration and analysis "on incidents, threats and emerging risks." Less than two months later the Metcalf attack occurred. In December the administration published the third NIPP.

2014: In response to a FERC order stemming from the Metcalf attack, NERC created Critical Infrastructure Protection 014 standard.

2015: As an extension to the 2013 NIPP, the administration releases an Energy Sector-specific critical infrastructure protection program, lead by the Department of Energy and assisted by the Department of Homeland Security.

2018: President Donald Trump signs into law the Cybersecurity and Infrastructure Security Agency Act (CISA) of 2018. This transformed the NPPD into an agency-level entity within the Department of Homeland Security with a mandate to protect critical infrastructure.

2022: FERC approves the latest update to NERC's Critical Infrastructure Protection 014 standard.

Sources: Federation of American Scientists, Cybersecurity and Infrastructure Security Agency, Computer Security Online, Congressional Research Service, White House, Advancing Security Worldwide, Department of Energy,

Political momentum increased after FERC briefed congressional leaders in June 2013 on the results of a power-flow analysis. (A power-flow analysis, also called a load-flow analysis, is used in power system operation and planning to assess how electricity moves within an interconnected system, like a transmission grid, and at what magnitudes.[26]) FERC officials "identified less than 100 critical high voltage substations on (the) grid that need to be protected from a physical attack."[27] However, results from their power-flow analysis showed that if malicious actors were able to destroy just nine of these critical substations, along with a transformer manufacturer, then "the entire United States grid would be down for at least 18 months, probably longer."[28]

Following the Metcalf attack and the subsequent power-flow analysis undertaken by government officials, FERC issued an order to NERC on March 7, 2014, to create, promulgate, and implement physical security standards for grid transmission infrastructure. In response, NERC created Critical Infrastructure Protection 014 (CIP 014), which outlines physical reliability standards to protect facilities against any hazards that would render them inoperable or otherwise severely damage them.[29] Revised versions of the standards were approved in November 2014 and most recently in 2022, after reviews by FERC. A report by NERC found that although the most recent version, CIP-014-3, is meeting its overall objectives, the organization is currently evaluating possible changes to provide clarity on how risk assessments are best performed by utility companies to determine whether or not an asset is designated a "critical substation" under the standard.[30] CIP-014 is the primary NERC standard for physical security, though other relevant standards include CIP-001 (reporting disturbance/unusual activity), CIP-004 (personnel integrity and training), CIP-006 (physical security perimeter management), CIP-008 (incident response/response planning), and CIP-009 (disaster recovery planning).[31]

A 2017 study by the U.S. Government Accountability Office identified 12 unique efforts by federal departments and agencies to enhance the security of the transmission grid against physical attacks.[32] These various efforts cut across three coexisting approaches to enhancing transmission grid physical security by government and private actors described in a 2018 report by the Congressional Research Service:

- **Hardening:** This describes a mixture of efforts that seek to prevent a successful attack from occurring. NERC's CIP-014 standard would fall within this approach. Measures include "monitoring critical facilities to identify would-be attackers before they attempt an attack, preventing attacker access to critical assets, and otherwise hardening facilities to make them more physically secure to protect against attack and equipment failure."[33]
- **Resilience:** These are efforts focusing on rapid recovery in the immediate aftermath of an attack and mitigating the overall effects of a successful attack. NERC's CIP-008 and CIP-009 would be categorized within this line of effort. In general, resilience efforts involve actions that augment the ability to "manage loads, reroute power flows, and access other sources of generation to reduce the potential of blackouts even if critical assets are disabled."[34]
- **Information sharing:** Risk reduction measures – whether hardening, resilience, or both – are directly informed by knowledge about existing and future threats from malicious actors. In practice, this mostly occurs through the secure online information portal Electricity Information Sharing and Analysis Center (E-ISAC). Established in 1998, E-ISAC is organizationally housed under NERC, but is separate from NERC's standards enforcement components. Although primarily used by NERC staff and its public utility company members, E-ISAC also has a Physical Security Advisory Group that includes representatives from U.S. governmental entities, such as the DOE and DHS. Finally, in addition to sharing threat information and providing situational awareness, E-ISAC hosts an annual security conference, GridSecCon, and a biennial tabletop exercise, GridEx, which assesses sector-wide responses to cyber and physical attacks. E-ISAC hosted its most recent GridSecCon on Oct. 17-20, 2023,[35] and ran GridEx VII on Nov. 14-15, 2023.[36]

Violent Far-Right Extremist Targeting of the Electrical Sector

Threat Assessment Overview

As a result of online discussions among movement supporters,[37] recent terrorist plotting arrests, and attack capability, the authors assess that violent far-right extremists are the most likely DVEs to physically attack the transmission grid. The end goal for violent far-right extremists is to overthrow the existing sociopolitical order and replace it with what they consider a utopian society (e.g., a white ethnostate or idealized version of the early American Republic).

While the likelihood of achieving such a goal is small, especially given that far-right attacks are frequently associated with lone actors and small group structures (as opposed to large formal organizations like al Qaeda and the Islamic State), violent actors believe that strategically executed attacks on key targets, including critical infrastructure, can make this dream a reality. At minimum, violent far-right actors can strategically benefit from such attacks by sowing social unrest, deepening existing polarization within and between communities, and undermining public confidence in governmental actors through disrupting their ability to effectively to respond to emergencies, including electrical power disruption (both localized and regionally).

Within the ideologically diverse U.S. violent far-right milieu, the two submovements with violent actors collectively demonstrating the greatest intent and capacity to carry out physical attacks against the transmission grid are white supremacists and militia extremists. Their well-established record of extensive possession of and training with caches of firearms, incendiaries, and explosives[38] indicates that violent far rightists will continue to favor physical attacks against transmission grid targets over cyberattack options in the near to mid future. Their most likely means of attempting physical attacks against the electrical sector will be shootings, arson, and bombings. There is some preliminary evidence to suggest that far-right extremists, particularly white supremacists, may seek to use innovative methods of attack, such as the incorporation of aerial drones in their attack planning and execution.

Further, U.S. violent far-right extremists have also demonstrated some interest and capability in conducting cyberattacks,[39] though there is no known evidence to suggest prior or current interest in specifically targeting the transmission grid. However, future use of cyberattacks by violent far rightists, especially militant accelerationist neo-Nazi and Boogaloo Bois (within the white supremacist and militia extremist movements, respectively) cannot be ruled out. (In the context of violent extremism, militant accelerationism can be defined as the belief in using violence in furtherance of a strategy to hasten the collapse and replacement of an existing government and underlying social order.[40])

Actors within both submovements, to varying degrees, are involved online and actively present in cyberspaces with high levels of illicit/illegal activity like the dark web and the encrypted social media messaging platform Telegram, among a host of other online platforms.[41] Cyber intelligence firms have repeatedly warned about online illegal marketplaces shifting toward cheaply selling malware and infected hardware services (known as Malware-as-a-Service and Infrastructure-as-a-Service, respectively). One forecasted outcome of these emerging business models is that their availability "reduces the technical skills requirement for advanced attacks, allows cybercriminals to scale their operations without added effort, and challenges network defender responses and attribution."[42] This potential threat is compounded by the growing adoption of artificial intelligence and machine learning techniques to create malware and execute cyberattacks.[43] While we do not predict a sudden rise in far-right-executed (or purchased) cyberattacks against the electric grid in the near term, it is not improbable that future attacks could begin simultaneously using physical and cyber strategies to attack targets, with the latter set of actions facilitated by Malware-as-a-Service and Infrastructure-as-a-Service purchased from illicit/illegal online vendors.

Finally, insofar as threats to personnel are concerned, there is currently no evidence suggesting

that far-right extremists are targeting transmission grid workers for fatal violence. White supremacists and, to a lesser degree, militia extremists are not averse to generating fatalities. Nevertheless, far-right violence against the electrical sector has thus far not been directed at personnel because first, these targets are soft (for example, they are physically remote and unattended) and second, these actors have an operational interest in temporarily avoiding casualties to avoid law enforcement attention.[44] Currently, there are also no known cases of far-right insider threats within the transmission grid sector. The lack of research on this topic calls into question the reliability and confidence of any assessment currently. However, this is an issue that, while not substantiated at present, cannot be dismissed as unlikely, either, given that other parts of the energy sector have been infiltrated by far-right extremists before.[45]

White Supremacists

White supremacist interest in targeting the transmission grid is influenced by several factors. For decades, movement figureheads and ideologues have advocated for carrying out attacks using small cells and lone offenders under a general operational philosophy of "leaderless resistance."[46] While eschewing formal organizational structures is intended[47] to increase operational security against infiltration from law enforcement, it also increases the difficulty of engaging in operationally sophisticated attacks, especially against hardened targets.[48] Not surprisingly, white supremacists, who typically operate outside the sphere of influence of large, formal organizations, tend to favor small-scale attacks against lightly defended soft targets,[49] including the transmission grid.[50]

Recently, U.S. far-right extremists have been experimenting with aerial drones for the purpose of spreading propaganda.[51] However, violent Russian far rightists participating in the conflict in Ukraine have made malevolent innovations that could influence their American counterparts to gradually incorporate the use of drones for intelligence, surveillance, and reconnaissance or as a weapon delivery mechanism.[52] Violent far-right and white supremacist experiments with innovations are likely to be further enabled by their embrace of additive manufacturing (3D printing) practices[53] and

Recent Cases of White Supremacists Targeting of the Electrical Sector

- **October 2020:** Three white supremacists from Idaho were charged with conspiracy to unlawfully manufacture, possess, and distribute various firearms and firearm accessories.
- **November 2020:** A North Carolina man was charged with firearms and interstate shipping violations.
- **June 2021:** A fifth individual in New Jersey was also arrested and accused of supplying untraceable firearms to the other men.
- **August 2021:** Four of the men were charged with conspiracy to damage property of a U.S. energy facility. They reportedly discussed at length a previous attack on power infrastructure by an unknown group, using assault-style rifles.
- **December 2020:** A white supremacist teen was arrested for plotting to conduct a shooting attack on the electrical grid in the southeastern U.S. The teenage suspect wanted to be "operational for violence" by the 2024 presidential election because they believed a Democrat would win.
- **February 2022:** Three white supremacists from Ohio, Wisconsin, and Texas pleaded guilty "related to a scheme to attack power grids in the United States in furtherance of white supremacist ideology." According to media reports, the suspects were attempting to incite a race war by carrying out shooting attacks on electrical substations.
- **January 2023:** A leading figure within the neo-Nazi white supremacist group Atomwaffen Division, originally from Florida, was arrested for plotting to attack the power grid in Baltimore, Maryland, along with a second suspect, also a neo-Nazi supporter, who was also arrested in Maryland.

Sources: Federation of American Scientists, Cybersecurity and Infrastructure Security Agency, Computer Security Online, Congressional Research Service, White House, Advancing Security Worldwide, Department of Energy,

general engagement with jihadist online content,[54] including technical manuals and operational practices.[55]

An additional source of ideational influence, particularly for those influenced by militant accelerationist ideas, is the belief in a grand strategy[56] of overthrowing the U.S. government and replacing it with a white ethnostate, generating mass fatalities in the process. The specific logic behind targeting transmission grids within this grand strategy is that electricity outages will instigate violent civil unrest and paralyze government responses from police, firefighters, and emergency medical services. The ensuing chaos is expected to spread like a contagion and provoke a wider race war between whites and nonwhites throughout the country. In turn, this will lead to the collapse and replacement of the federal government with a fascistic racial dictatorship, inspired by the example of Nazi Germany.

Finally, beyond militant accelerationism, many white supremacists are also motivated by beliefs and perceptions such as racism, antisemitism, or anti-LGBTQ+ hostility, as well as fears over immigration, changing demographics, and inclusive[57] multiculturalism. Thus, while there are literally tens of thousands of potential targets to choose from, some violent actors interested in targeting the electric grid have plotted against transmission and distribution infrastructure serving population centers with high concentrations of minority residents.[58] Some are additionally motivated by a resurgent far-right philosophy called eco-fascism, which can be described as groups or individuals who combine strong environmentalist beliefs (e.g., "deep ecology") with fascist views to advocate a variety of criminal behaviors, including violence.[59] Attacks on energy sector infrastructure (and people perceived to be enemies of whites[60]), including the transmission grid, are thus also seen as a defense of the environment, in addition to being perceived by movement actors as advancing the supremacy of whites.

Militia Extremists

Militia extremists also continue to show interest in targeting the transmission grid. Broadly speaking, militia extremists' interest in attacking the transmission grid is directly connected to their hatred of the government. Parallel to how many white supremacists advocate for a race war, some militia extremists have also targeted the transmission grid in the hope of instigating a civil war with what they believe are unpatriotic Americans who are attempting to exercise tyrannical government control over patriotic citizens.[61]

Many also share other intermediate motives with white supremacists, like the desire to both exploit and cause widespread panic[62] leading to civil unrest, undermining public trust in government, as well as attempting to overthrow the government by force.[63] (In the case of the militant accelerationist Boogaloo submovement, the end goal is an idealized form of the early American Republic rather than an explicitly racist white ethnostate.[64]) Largely due to early law enforcement interdiction, much of the past attack plotting did not materialize.

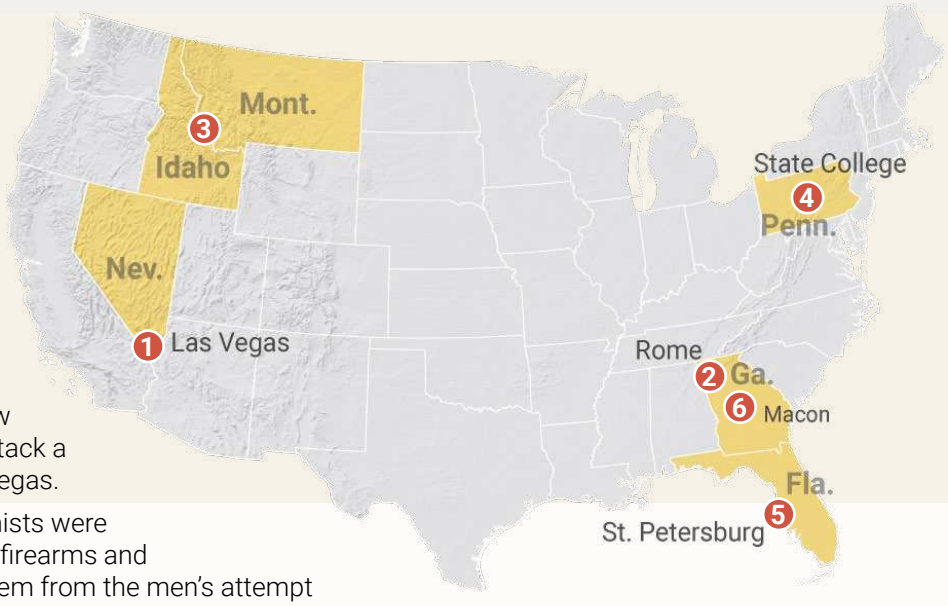
Violent Far-Left Extremist Targeting of the Electrical Sector

Threat Assessment Overview

The three main subsets of actors among far-left extremists most likely to target the transmission grid are violent eco-extremists, violent left-wing anarchist extremists, and violent far leftists primarily motivated by social causes. Violent far-left extremists have had a long history of targeting critical infrastructure, with attacks against transmission grid infrastructure documented as early as 1970.[65] However, there have been no confirmed cases of violent far-left attacks against the transmission grid since 2003. Should they consider resuming attacks against the transmission grid in the near term, we assess violent far-left extremists will continue to favor physical attacks against transmission grid infrastructure. We base this judgment on technical and operational simplicity of such attacks relative to other methods (i.e., cyber), familiarity with physical attack methods (as observed by the publication and content of attack tradecraft manuals),[66] and ideological beliefs.

Far-left actors utilize a wide range of "direct action" tactics and strategies that range from nonviolent to violent in terms of practice and from lawful to unlawful in terms of legality.[67] Physical attacks, should they resume in

Prominent Militia Extremist Cases Related to the Energy Sector



1. May 30, 2020: Three Boogaloo Bois militia extremists were arrested on firearms and explosives charges in Las Vegas, Nevada, during ongoing civil unrest. The men reportedly were observed filling gas cans in a parking lot near the civil unrest and making Molotov cocktails using glass bottles. These men were charged with conspiracy to damage or destroy by fire and explosive and possession of unregistered firearms. A criminal affidavit also describes how the men may have been plotting to attack a local public utility installation in Las Vegas.

2. Feb. 15, 2014: Three militia extremists were arrested in Rome, Georgia, on federal firearms and explosives violations. The charges stem from the men's attempt to obtain pipe bombs and other explosives for use in guerilla-style attacks to sabotage power grids, electricity transfer stations, and water treatment facilities.

3. Aug. 31, 2005: Authorities arrested and charged a suspect for a string of burglaries and vandalism incidents throughout Idaho over a two-month period. The suspect, David Pruss, who was known to locals for expressing strong far-right antigovernment views and having ties to militia groups in Idaho and Montana, caused more than $100,000 in property damage to power transformers, a small hydro-electric dam, and logging equipment.

4. June 19, 2002: Federal law enforcement authorities arrested a militia extremist and charged him with unlawful manufacturing and possession of explosive devices as well as illegal firearms. During a search of the suspect's residence in State College, Pennsylvania, investigators found three fully automatic assault rifles, two hand grenades, an illegal firearms silencer, and two 30-pound mortar shells wrapped with lead pellets serving as shrapnel.Officers also found blueprints of the Penn State University's electrical system, among other items.

5. Dec. 8, 1999: A suspected militia member was arrested on conspiracy to attack critical infrastructure and possible firearms violations near St. Petersburg, Florida. The suspect, who is described as the leader of a militia coalition called the "Southeastern State Alliance" was charged with conspiring to burglarize National Guard armories for purpose of obtaining explosives to bomb transmission towers and high voltage transmission lines in Florida.

6. April 26, 1996: Three militia extremists who were members of the Georgia Republic Militia were arrested in Macon, Georgia, for various firearms and explosives violations. Federal authorities surmised they were plotting to attack roads, bridges, and power lines.

Sources: Federation of American Scientists, Cybersecurity and Infrastructure Security Agency, Computer Security Online, Congressional Research Service, White House, Advancing Security Worldwide, Department of Energy,

the near term, are most likely to manifest in arson attacks and so-called monkey wrenching – acts of sabotage such as cutting wires or removing screws, nuts, and bolts from support structures. Based on prior usage against perceived adversaries, violent far leftists may incorporate commercially available technological innovations such as the use of aerial drones for intelligence, surveillance, and reconnaissance purposes.[68]

Compared to violent far-right extremists, far-left extremists pose a smaller, but nontrivial, potential threat of physical attacks against the transmission grid. There are two overarching reasons for this. First, although historically violent far-left extremists were the primary perpetrators of ideologically motivated attacks on the power

grid,[69] this is no longer the case. During the 1990s and into the early 2000s, violent eco-extremists, violent left-wing anarchists, and other violent far leftists carried out attacks against the transmission grid, but there have been no known physical attacks or plots targeting the transmission grid by violent far-left extremists in the U.S. since then.

Second, there are important qualitative strategic differences between far-right and far-left attacks. Whereas the former set of actors tend to attack critical infrastructure as part of a wider goal that will deliberately generate fatalities (race war/civil war, overthrow of U.S. government, etc.), the latter has sought to deliberately avoid fatalities in furtherance of publicizing issues related to corporate profit-making and its perceived impacts on human beings and the ecosystem.[70]

That said, despite what appears to be a present lull in physical attacks against the transmission grid by far-left extremists, renewed targeting of electrical distribution and transmission infrastructure remains a possibility. Violent extremists leverage ongoing environmental issues such as climate change and continued use of fossil fuels to inspire and mobilize supporters into violence. Violent far-left extremists continue to maintain the capability to conduct sabotage attacks. They continue to carry out physical violence against infrastructure in North America,[71] including against the energy sector assets in the United States,[72] and could be persuaded to strike the transmission grid again. Moreover, far-left actors have made statement condoning and glorifying attacks against critical infrastructure, including sabotage to Canadian parts of the North American electric grid, as recently as 2017.[73]

While U.S. violent far-left extremists have demonstrated interest and capability in conducting cyberattacks,[74] there is no known evidence from open sources to suggest prior or current interest in specifically cyberattacking the transmission grid. In terms of capabilities, far-left actors have publicly posted guidance on hacking the phones of politicians like Donald Trump[75] and carried out digital intrusions and information theft,[76] denial-of-service attacks, and website defacement.[77] This record of attacks suggests that violent far leftists have supporters and resources within hacking communities that they can draw upon for cyberattacks. If prior history of physical attacks against transmission grid infrastructure is any indication, some violent far leftists may see power grids as a potentially attractive cyber target.

Nevertheless, the violent far-left actors' general commitment to avoiding fatalities could dampen any potential attractiveness of cyberattacks.[78] Whereas physical attacks against transformer and distribution infrastructure are most likely to result in limited disruption (unless targeting critical substations, as noted earlier), well-designed cyberattacks can lead to widespread blackouts,[79] affecting medical and other emergency response services. Given their ongoing commitment to avoiding fatalities, violent far leftists would likely be aware of such potential consequences when weighing when, where, how, and whether to attempt a cyberattack.

Finally, violent far leftists seem to pose a low threat level to transmission grid personnel in terms of fatal violence. Their past aversion to casualties makes targeting workers and managers for physical violence unlikely, despite past rhetoric from some actors suggesting otherwise.[80] Moreover, given their typically anti-corporate and often anti-capitalist belief systems, they are unlikely to present themselves as insider threats who enter the workforce with the intent of infiltration. However, the possibility of an individual joining the workforce and then later becoming radicalized and becoming a violent far-left insider cannot be dismissed.[81]

Violent Ecological Extremists

Between 1996 and 2006, violent ecological extremists conducted hundreds of criminal acts causing at least $100 million in damage to a wide range of businesses that movement supporters deemed guilty of destroying the environment.[82] Past violent environmental extremist direct action campaigns against targets, including the transmission grid, have encompassed verbal and physical altercations with police and security staff, directly expressed threats, vandalism, and sabotage acts using monkey wrenching techniques and arson.[83] They demonstrated a repeated desire and willingness to attack electrical infrastructure

A worker repairs damage following an attack on power substations in Carthage, N.C., in December 2022. (Peter Zay / Anadolu Agency via Getty Images)

in the United States, specifically targeting electric power-generating facilities as well as high-voltage transmission line towers.[84] An illustrative example is when four supporters of the Earth Liberation Front and Animal Liberation Front movements worked together to attack and topple an 80-foot electric transmission tower outside of Bend, Oregon, on Dec. 30, 1999. While the attack did not disrupt electrical service to local residents and businesses, it caused an estimated $126,000 in property damage.[85]

Left-Wing Anarchist Extremists

Left-wing anarchist extremists have also engaged in various ideologically motivated attacks against various forms of critical infrastructure, including the transmission grid. These attacks have primarily involved acts of monkey wrenching and other forms of sabotage. Some of these actors can be described as "green" left-wing anarchists, in which they meld their deep philosophical rejection of any government and capitalism with radical ecological beliefs shared by environmental extremists. Others have been motivated by anti-authority beliefs and personal impulses,[86] validated by anarchist ideologies.

Other

In a throwback to ideological currents prevalent in the 1970s and 1980s, rather than being primarily motivated by ecological concerns and/or a deeper philosophical rejection of all government, some far-left extremists may be motivated to attack transmission grid infrastructure in furtherance of various social causes such as racial justice movements, socioeconomic concerns, and/or anti-war beliefs.

Some prominent violent far-left cases targeting the electrical sector include:

- On Nov. 2, 2003, a person with far-leftist views was arrested for sabotage incidents involving the removal of bolts anchoring high-voltage transmission towers to their concrete platforms in Washington, Oregon, and California. Court proceedings revealed he engaged in sabotage attacks against "more than 20" towers. Some of the towers toppled to the ground, causing a localized power outage. The suspect stated that he wanted to draw attention to potential vulnerabilities of America's power grid being overlooked amid what he viewed as heavy-handed counterterrorism measures after 9/11.[87]
- Between June 1998 and January 2001, a self-described violent anarchist carried out a series of vandalism attacks against power substations, causing 28 power failures and 20 service disruptions in Wisconsin.[88] The suspect also possessed cyanide, a potentially lethal chemical agent,[89] but he claimed he contemplated using it to kill himself.[90] He served 17 years in custody, including 13 years in federal prison before being released in 2020 under supervision for the next five years.[91]

Policy Recommendations

To guard against and mitigate potential DVE threats and attacks against the U.S. electrical sector, government policymakers should consider these recommendations:

- Update practices related to insider threats. Some attacks against electrical substations and transformers suggest possible insider knowledge of critical equipment to target, even as the perpetrators and their motives remain elusive.[92] As noted in the Threat Assessment Overviews in this report, insiders posing physical threats to assets are within the realm of possibility. Investigative reporting has identified extremist infiltration and recruitment within other parts of the energy sector; the authors' research has surveyed and assessed far-right insider threats across multiple U.S. government departments and agencies.[93]
- The scarce research and recommended practices for insider threats within the energy industry are dated, focus mainly on information security, and – to the extent they address physical threats from violent extremists – advocate for questionable practices. For example, a report from DHS' National Infrastructure Advisory Council, dated from 2008 and cited in later research on energy sector security,[94] among other things, advocated for utility companies having some employees and job candidates vetted through the Terrorism Screening Center's database.[95] This is not only extremely problematic from a privacy, civil rights, and civil liberties standpoint,[96] but is also ineffective at preventing threats posed by DVE actors, such as violent far-right extremists who attacked the U.S. Capitol complex on Jan. 6, 2021.[97]
- Instead, we recommend that employee vetting and other insider risk and insider threat mitigation practices should be centered on standard criminal background checks, clear workplace conduct standards, carefully designed and implemented employee reporting practices,[98] established behavioral observation programs,[99] and a robust social media policy that is consistent with all applicable state and federal guidelines and laws.[100] NERC's critical infrastructure program standards contain guidance for addressing cyber-related insider threats; it is unclear how applicable they are to physical attack-related insider threats. We recommend policymakers review existing standards and where applicable, close any potential gaps related to physical attack-related insider threats, informing updated guidance based on lessons learned from "best practices"[101] and "worst practices."[102]
- Improve planning for future threats. Citing FERC research, one study found that utilities and systems operators' standard contingency planning is insufficient to address an operationally sophisticated attack by terrorists.[103] FERC and NERC should update their contingency planning and incorporate assessments based on terrorist attack scenarios involving recent malevolent innovations and trends such as weaponized aerial drones and utilization of cyberattacks in simultaneous combination with physical attacks.
- Expand data-driven approaches to risk assessment and resource allocation. While NERC's CIP-014-3 is an adequate standard for identifying and protecting the most critical substations, it represents a small fraction of a wider set of less critical, but highly vulnerable, assets like the substations attacked in Moore County, North Carolina, which left tens of thousands of customers without power for several days, prompting a countywide state of emergency and temporary curfew.[104] Examples from recent ideologically motivated attacks against the transmission grid suggest that aside from fulfilling ideological goals, specific targets are chosen based on geographic proximity to where offenders live and/or what demographics are served. E-ISAC currently provides event-driven analyses to its consumers. It should also develop analytic products that can proactively inform utility companies' situational awareness about DVE threats, such as utilizing open-source information on malevolent actors advocating violence and expressing interest in attacking transmission and distribution assets.
- Without ignoring other potential threats and risks, immediate analytic priority should be given to threats from violent

> “Notwithstanding that far-left and far-right DVEs will continue to favor physical attacks in the near term, developments in technology, illicit/illegal marketplaces, and malevolent innovations suggest that would-be adversaries may adopt new attack methods.”

far-right actors, given their ongoing activity and wider goals. Security efforts should include substations that fall just below the threshold of “critical” in CIP-014-3 and that are geographically proximal to known locations of extremist actors engaging in behaviors like bomb making, weapons training, and paramilitary mobilization.

- Support further research on violent extremist targeting of critical infrastructure, including electrical sector assets and personnel. While there has been notable progress recently, there are still many gaps in the research on critical infrastructure protection. Among other things, consideration for future research should include additional data on attack patterns against transmission grid infrastructure by a broad array of ideologically motivated actors,[105] as well as research into insider threat practices within public utility and other energy companies.[106]

Ongoing Challenges

White supremacists and militia extremists are currently the greatest threat to the electrical sector. Militia extremists and white supremacists are known to possess the capability to carry out a large-scale, mass casualty-producing event, and may use such capability in the future against a variety of targets, including the electrical sector. As a result, violent far-right extremist attacks against the electrical sector will likely involve shooting attacks, arson, and possibly bombings.

In contrast, violent far leftists pose a smaller, but not negligible, threat to the electrical sector and have been known to carry out actual physical attacks against high-voltage transmission towers and power lines. However, they have generally lacked the willingness to kill or harm people and have not demonstrated the violent capability to carry out a large-scale terrorist attack against a hardened target. The potential criminal actions of violent environmental extremists and green anarchists against the electrical sector, should they occur, will likely be limited to criminal acts of civil disturbance, vandalism, arson, sabotage, and the like. That said, violent far-left extremist interest in renewing attacks against the power grid should not be discounted, due to ongoing environmental issues such as climate change and the continued use of fossil fuels to generate electricity.

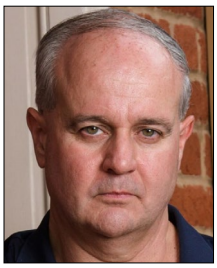
Notwithstanding that far-left and far-right DVEs will continue to favor physical attacks in the near term, developments in technology, illicit/illegal marketplaces, and malevolent innovations suggest that would-be adversaries may adopt new attack methods. These include easier access to cyberattack methods and use of aerial drones in attack planning and execution. The possibility of an insider threat, while uncertain given the lack of data, is not something that can be easily dismissed at this time, either.

Current events surrounding concerns over global population growth, unauthorized immigration flows, current “culture war” controversies targeting members of the LGBTQ+ community, climate change and destruction of the environment, and perceived corporate greed are having an enduring impact on both violent far-right and violent far-left extremist mobilization in the U.S. These issues may increase their respective interests in attacking the electrical sector. Further, the electrical sector and society’s dependence on it makes it a

lucrative target to cause societal chaos, thus undermining the public's trust in government, resulting in widespread civil disturbance and potential loss of governmental control and civil order. For this reason, the U.S. government and nongovernment actors with vested interests in the security of the energy sector are encouraged to bolster physical security measures at electric power-generating facilities, electric substations, and larger electric transfer locations in addition to bolstering information-sharing efforts. Together, they must remain vigilant to possible DVE activity targeting the electrical sector, including potential threats (both real and intended), and relevant arrests or disrupted plots against other, similar kinds of critical infrastructure.

Lastly, law enforcement operations against DVEs have proved successful at preventing acts of terrorism against the electrical sector. Conversely, these operations and subsequent prosecutions have also alerted DVEs to adopt better operational security measures using small cell and lone offender practices.[107] As a result, DVEs are likely determined to continue their pursuit of targeting and attacking the electrical sector for the foreseeable future. Monitoring DVE networks and disrupting these plots before they result in harmful damage must be a priority for intelligence, law enforcement, and the private sector nationwide. ☐

Alejandro J. Beutel is a nonresident fellow with the New Lines Institute for Strategy and Policy who studies non-violent and violent far-right extremist and Islamist movements. Beutel is a former Senior Research Analyst at the Southern Poverty Law Center and a former Researcher for Countering Violent Extremism at the University of Maryland's National Consortium for the Study of & Responses to Terrorism. He is also a doctoral student in Criminology and Justice Studies at the University of Massachusetts Lowell.



Daryl Johnson is one of the foremost experts on domestic extremist groups in the United States and a nonresident fellow with the New Lines Institute for Strategy and Policy. Beginning his career as a civilian in the U.S. Army, Johnson has held several government positions, most recently as senior analyst at the Department of Homeland Security. He is also regularly cited, featured, or quoted in media covering domestic extremist groups in the United States, including the New York Times, Washington Post, Wall Street Journal, Newsweek, National Public Radio, MSNBC, CNN, and NBC Nightly News, among many others. He is the author of "Hateland: A Long, Hard Look at America's Extremist Heart" (Prometheus Books, 2019) and "Right-Wing Resurgence: How a Domestic Terrorism Threat Is Being Ignored" (Rowman & Littlefield, 2012).

Endnotes

1 Loadenthal, M. (2021, January 19). *Anti-5G, infrastructure sabotage, and COVID-19*. Global Network on Extremism & Technology. Retrieved September 18, 2023, from https://gnet-research.org/2021/01/19/anti-5g-infrastructure-sabotage-and-covid-19; Loadenthal, M. (2021, February 15). *Infrastructure, sabotage, and Accelerationism*. Global Network on Technology & Extremism. Retrieved September 18, 2023, from https://gnet-research.org/2021/02/15/infrastructure-sabotage-and-accelerationism/; Loadenthal, M. (2022). Feral fascists and deep green guerrillas: Infrastructural attack and accelerationist terror. *Critical Studies on Terrorism*, *15*(1), 169–208. https://doi.org/10.1080/17539153.2022.2031129.

2 When mentioning the term "ideology," the authors are referencing it in the context of a violent extremist ideology. Drawing upon the work of Gary Ackerman, Michael Burnham, and Jeffery Bale, we define a violent extremist ideology as a set of beliefs enunciated by nonstate actors that justifies the intentional use or threatened use of violence against targets that are chosen for their symbolic and/or representative value to manipulate the attitudes and behavior of a wider target audience by instilling anxiety. Ideologies can contain beliefs that are formulated as conspiracy theories. The authors' definition of a "conspiracy theory" is borrowed directly from Karen Douglas and Robbie Sutton: "a belief that two or more actors have coordinated in secret to achieve an outcome, and that their conspiracy is of public interest, but not public knowledge." When referring to "extremist narratives," we borrow directly from Scott Ruston: "a system of stories that hang together to provide a coherent view of the world for the purpose of supporting individuals, groups, or movements to further illegal violent and violence-assisting activities." From these definitions, ideologies and conspiracy theories provide the ideational basis for narratives. Extremist narratives are a systematic storytelling "vehicle" to transform and repetitively

communicate the underlying ideas of ideologies and conspiracy theories to wider audiences and enhance their persuasive appeal. See: Ackerman, G. A., & Burnham, M. (2019). Towards a definition of terrorist ideology. *Terrorism and Political Violence*, *33*(6), 1160–1190. https://doi.org/10.1080/09546553.2019.1599862, citing, with modifications, Ackerman, G., Abhayaratne, P., Bale, J., Blair, C., Hansell, L., Jayne, A., Kosal, M., Lucas, S., Moran, K., Seroki, L., & Vadlamudi, S. (2006, December 4). *Assessing terrorist motivations for attacking critical infrastructure* (UCRL-TR-227068). Lawrence Livermore National Laboratory. https://www.osti.gov/servlets/purl/902328; Douglas, K. M., & Sutton, R. M. (2023). What are conspiracy theories? A definitional approach to their correlates, consequences, and communication. *Annual Review of Psychology*, *74*(1), 271–298. https://doi.org/10.1146/annurev-psych-032420-031329; Ruston, S. W. (2009, September 3). Understand what narrative is and does. *Arizona State University Center for Strategic Communication*. https://csc.asu.edu/2009/09/03/understand-what-narrative-is-and-does/

3 For example, see: Baird, W. H. (2021). Measuring the balance of the world's largest machine. *American Journal of Physics*, *89*(12), 1086–1093. https://doi.org/10.1119/10.0005989; Aggarwal, S. (2014, November 24). *Greasing the electric grid, the world's largest machine (op-ed)*. LiveScience. Retrieved September 18, 2023, from https://www.livescience.com/48893-improving-efficiency-on-the-electric-grid.html; Cohn, J. A. (2018). *The grid: Biography of an American technology*. MIT Press; Stenvig, N. (2020, February 27). Nils Stenvig: Exploring the world's largest machine. *Oak Ridge National Laboratory*. https://www.ornl.gov/blog/nils-stenvig-exploring-worlds-largest-machine; Independent Electric System Operator. (2020, February 28). The world's largest machine: The North American power grid. *Powering Tomorrow Podcast* [SoundCloud podcast]. https://www.ieso.ca/en/Powering-Tomorrow/2020/The-Worlds-Largest-Machine-The-North-American-Power-Grid; TedEd. (2022, October 6). *What does the world's largest machine do? - Henry Richardson* [Video]. YouTube. https://youtu.be/YomAHwuuQEI

4 Cai, M., Douglas, E., & Ferman, M. (2022, February 15). *How Texas' power grid failed in 2021 — and who's responsible for preventing a repeat*. The Texas Tribune. https://www.texastribune.org/2022/02/15/texas-power-grid-winter-storm-2021/

5 For example, see: Thompson, B. G., Swalwell, E., & Magaziner, S. (2023, February 21). *Thompson, Swalwell, Magaziner request briefing on threats to critical infrastructure from domestic violent extremists*. Committee on Homeland Security Democrats. https://web.archive.org/web/20230227200759/https://democrats-homeland.house.gov/news/correspondence/thompson-swalwell-magaziner-request-briefing-on-threats-to-critical-infrastructure-from-domestic-violent-extremists. For text of the letter, see: https://web.archive.org/web/20230223002458/https://democrats-homeland.house.gov/imo/media/doc/letter_to_dhs_electrical_facility_attacks.pdf

6 U.S. Department of Homeland Security & U.S. Federal Bureau of Investigation. (2023). *Joint Intelligence Bulletin: Disruption of two racially or ethnically motivated violent extremists to attack the US power grid*. https://mcpa.memberclicks.net/assets/NEWSLETTER/FINAL%20%28U--FOUO%29%20JIB%20-%20Disruption%20of%20Two%20Racially%20or%20Ethnically%20Motivated%20Violent%20Extremists%2002082023.pdf. Also see: Wilson, C., & Ryan, J. (2023, January 19). *FBI warns of neo-Nazi plots as attacks on northwest power grid spike*. Oregon Public Broadcasting. Retrieved July 21, 2023, from https://www.opb.org/article/2023/01/19/surge-in-oregon-washington-substation-attacks-as-fbi-warns-neo-nazi-plots/; Sganga, N. (2023, February 17). *DHS "very concerned" about white nationalist attacks on power grid*. CBS News. Retrieved July 21, 2023, from https://www.cbsnews.com/news/dhs-white-nationalist-attacks-power-grid/; Lambert, E. (2023, April 24). *DHS warns tactics shared online threaten electrical grid*. NewsNation. Retrieved July 21, 2023, from https://www.newsnationnow.com/us-news/infrastructure/dhs-warning-online-tactics-electrical-grid-threats/

7 Clarke, C., Saltskog, M., Millender, M., & Fink, N. C. (2023). The targeting of infrastructure by America's violent far-right. *CTC Sentinel*, *16*(5), 26–32. https://ctc.westpoint.edu/wp-content/uploads/2023/05/CTC-SENTINEL-052023.pdf; Krill, I., & Clifford, B. (2022). *Mayhem, murder, and misdirection: Violent extremist attack plots against critical infrastructure in the United States, 2016–2022*. Program on Extremism at George Washington University and NCITE. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/CriticalInfrastructureTargeting09072022.pdf

8 McBride, J., Siripurapu, A., Maizland, L., & Lieberman, E. (2021, May 13). *How does the U.S. power grid work?* Council on Foreign Relations. https://www.cfr.org/backgrounder/how-does-us-power-grid-work. On U.S.-Mexico cross-border transmission line connections, see: Andrade, D., Sweedler., A., Martin, J., Prieto, A., Rounds, K., & Gruenwald, T. (2022). Baja California Energy Outlook 2020-2025. Institute of the Americas. https://iamericas.org/wp-content/uploads/2022/02/Baja_Energy_Outlook_2020_2025.pdf, 13-14.

9 McBride, J., Siripurapu, A., Maizland, L., & Lieberman, E. (2021, May 13). *How does the U.S. power grid work?* Council on Foreign Relations. https://www.cfr.org/backgrounder/how-does-us-power-grid-work

10 National Research Council. (2012). *Terrorism and the Electric Power Delivery System*. Washington, D.C.: The National Academies Press. https://doi.org/10.17226/12050, p. 2; Miller, E. (2016). *Terrorist attacks targeting critical infrastructure in the United States, 1970-2015*. University of Maryland START Center. https://web.archive.org/web/20190430195710/https://www.start.umd.edu/pubs/DHS_I%26A_GTD_Targeting%20Critical%20Infrastructure%20in%20the%20US_June2016.pdf

11 U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency & U.S. Department of State Bureau of Counterterrorism. (2019). *A guide to critical infrastructure and resilience*. https://web.archive.org/web/20221026213322/https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf, p. 3.

12 This study was originally funded by DHS and completed in 2007, but approved for declassified publication in 2012. National Research Council. 2012. *Terrorism and the electric power delivery system*. Washington, D.C.: The National Academies Press. https://doi.org/10.17226/12050

13 Office of the Director of National Intelligence. (2021). *(U) Domestic violent extremism poses heightened threat in 2021*. https://web.archive.org/web/20210317191505/https://www.dhs.gov/sites/default/files/publications/21_0301_odni_unclass-summary-of-dve-assessment-17_march-final_508.pdf

14 For example, a 2016 study by the University of Maryland's START center examined terrorist attacks against multiple forms of critical infrastructure from 1970 to 2015. However, only a small portion of the study was dedicated to attacks against the transmission grid. Moreover, its temporal parameters mean its findings are slightly dated, with its most recent data at least eight years old. An August 2022 study published by George Washington University's Program on Extremism partially extends the START study to 2022, but like the University of Maryland study, only has a small portion of content focused on the transmission grid. Moreover, the study is focused on attacks from actors motivated by white supremacist and jihadist ideologies; the authors acknowledge that attacks from other actors like far-right militia extremists and far-left anarchist and eco-extremists are not discussed. Finally, a 2023 study published in the CTC Sentinel broadly surveyed recent attacks against U.S. critical infrastructure by far-right extremists. Like the other two studies, only a small portion, relative to the rest of the article, was dedicated to physical threats to the transmission grid. The article's scope also meant other DVE actors from the far-left were unaddressed. Clarke, C., Saltskog, M., Millender, M., & Fink, N. C. (2023).

The targeting of infrastructure by America's violent far-right. *CTC Sentinel*, *16*(5), 26-32. https://ctc.westpoint.edu/wp-content/uploads/2023/05/CTC-SENTINEL-052023.pdf; Krill, I., & Clifford, B. (2022). *Mayhem, murder, and misdirection: Violent extremist attack plots against critical infrastructure in the United States, 2016-2022*. Program on Extremism at George Washington University and NCITE. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/CriticalInfrastructureTargeting09072022.pdf; Miller, E. (2016). *Terrorist attacks targeting critical infrastructure in the United States, 1970-2015*. University of Maryland START Center. https://web.archive.org/web/20190430195710/https://www.start.umd.edu/pubs/DHS_I%26A_GTD_Targeting%20Critical%20Infrastructure%20in%20the%20US_June2016.pdf

15 According to the U.S. Department of Homeland Security, a "homegrown violent extremist" is: "A person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization (FTO), but is acting independently of direction by an FTO. HVEs are distinct from traditional domestic terrorists who engage in unlawful acts of violence to intimidate civilian populations or attempt to influence domestic policy without direction from or influence from a foreign actor." See: U.S. Department of Homeland Security. (2020). *Homeland threat assessment*. https://web.archive.org/web/20230703151300/https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf

16 Cooper, A., & Miller, J. (2023, February 4). *A vulnerable power grid is in the crosshairs of domestic extremist groups*. CNN. https://edition.cnn.com/2023/02/04/us/us-power-grid-attacks; Krill, I., & Clifford, B. (2022). *Mayhem, murder, and misdirection: Violent extremist attack plots against critical infrastructure in the United States, 2016-2022*. Program on Extremism at George Washington University and NCITE. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/CriticalInfrastructureTargeting09072022.pdf; Miller, E. (2016). *Terrorist attacks targeting critical infrastructure in the United States, 1970-2015*. University of Maryland START Center. https://web.archive.org/web/20190430195710/https://www.start.umd.edu/pubs/DHS_I%26A_GTD_Targeting%20Critical%20Infrastructure%20in%20the%20US_June2016.pdf

17 Hauck, G. (2023, March 15). *Power grid attacks caused outages for thousands. FBI still doesn't know who did it – or why*. USA Today. https://www.yahoo.com/news/power-grid-attacks-caused-outages-191851704.html; Hammond, C. (2023, May 1). *LGBT community says concerns in aftermath of Moore County protests go beyond a drag show*. Charlotte Observer. https://www.charlotteobserver.com/news/state/north-carolina/article269727816.html; Rahman, K. (2022, December 7). *Physical attacks on power substations in multiple states—Report*. Newsweek. https://www.newsweek.com/physical-attacks-power-substations-multiple-states-1765225

18 Memmott, M. (2014, February 5). *Sniper attack on Calif. power station raises terrorism fears*. National Public Radio. https://www.npr.org/sections/thetwo-way/2014/02/05/272015606/sniper-attack-on-calif-power-station-raises-terrorism-fears

19 ABC7. (2014, February 14). *Attack on South Bay power station called 'terrorism.'* https://abc7news.com/archive/9420318/.

20 Hauck, G. (2023, March 15). *Power grid attacks caused outages for thousands. FBI still doesn't know who did it – or why*. USA Today. https://www.yahoo.com/news/power-grid-attacks-caused-outages-191851704.html

21 Rusco, F., Ludwigson, J., Gaines, S., & Marroni, D. (2017). *Electricity: Federal efforts to enhance grid resilience* (GAO-17-15). United States Government Accountability Office. https://www.gao.gov/assets/690/682649.pdf. Also see: U.S. Department of Homeland Security. (2013). *NIPP 2013: Partnering for critical infrastructure security and resilience*. https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf

22 U.S. Department of Homeland Security & U.S. Department of Energy. (2015). *Energy sector-specific plan*. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf

23 Cybersecurity and Infrastructure Security Agency. (n.d.). *National infrastructure protection plan and resources*. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources

24 Rusco, F., Ludwigson, J., Gaines, S., & Marroni, D. (2017). *Electricity: Federal efforts to enhance grid resilience* (GAO-17-15). United States Government Accountability Office. https://www.gao.gov/assets/690/682649.pdf; Parfomak, P. W. (2018). *NERC standards for bulk power physical security: Is the grid more secure?* (R45135) Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45135

25 Smith, R. (2014, February 4). *Assault on California power station raises alarm on potential for terrorism*. Wall Street Journal. https://archive.vn/apOZW

26 Albadi, M. (2020). Power flow analysis. In K. Volkov (Ed.), *Computational models in engineering*. IntechOpen. https://doi.org/10.5772/intechopen.83374

27 Smith, R. (2014, March 12). *U.S. risks national blackout from small-scale attack*. Wall Street Journal. https://archive.vn/BVrbU

28 Smith, R. (2014, March 12). *U.S. risks national blackout from small-scale attack*. Wall Street Journal. https://archive.vn/BVrbU

29 North American Electric Reliability Corporation. (2022). *CIP-014-3 – Physical Security*. Retrieved July 21, 2023, from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-3.pdf?trk=public_post_comment-text. Also see: North American Electric Reliability Corporation. (2022, September 19). *ERO Enterprise CMEP Practice Guide Version 1.1, CIP-014-3 R1*. https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20CIP-014-3%20R1.pdf

30 North American Electric Reliability Corporation. (2023, April 14). *NERC announces actions addressing physical security*. https://www.nerc.com/news/Pages/NERC-Announces-Actions-Addressing-Physical-Security.aspx

31 For a concise overview, see: RSI Security. (2018, November 5). *NERC CIP standards: What you need to know*. https://blog.rsisecurity.com/nerc-cip-standards-what-you-need-to-know/; and RSI Security. (2023, March 18). *NERC CIP standards summary: All mandatory requirements, explained*. https://blog.rsisecurity.com/nerc-cip-standards-summary-all-mandatory-requirements-explained/

32 Rusco, F., Ludwigson, J., Gaines, S., & Marroni, D. (2017). *Electricity: Federal efforts to enhance grid resilience* (GAO-17-15). United States Government Accountability Office. https://www.gao.gov/assets/690/682649.pdf

33 Parfomak, P. W. (2018). *NERC standards for bulk power physical security: Is the grid more secure?* (R45135) Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45135, p. 19

34 Parfomak, P. W. (2018). *NERC standards for bulk power physical security: Is the grid more secure?* (R45135) Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45135, p. 19

35 Electricity Information Sharing and Analysis Center. (n.d.). *GridSecCon: The E-ISAC's annual security conference*. Retrieved November 2, 2023, from https://www.eisac.com/s/gridseccon

36 Parfomak, P. W. (2018). *NERC standards for bulk power physical security: Is the grid more secure?* (R45135) Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45135, p. 19-20. Also see: Brown, L. (2022, August 24). *E-ISAC overview*. Electricity Information Sharing and Analysis Center. https://www.wecc.org/Administrative/Brown-WECC%20CSWG%20Briefing.pdf.

37 For example, within the scholarly and grey literature, see: Loadenthal, M. (2021, January 19). *Anti-5G, infrastructure sabotage, and COVID-19*. Global Network on Extremism & Technology. Retrieved September 18, 2023, from https://gnet-research.org/2021/01/19/anti-5g-infrastructure-sabotage-and-covid-19; Loadenthal, M. (2021, February 15). *Infrastructure, sabotage, and accelerationism*. Global Network on Technology & Extremism. Retrieved September 18, 2023, from https://gnet-research.org/2021/02/15/infrastructure-sabotage-and-accelerationism/; Loadenthal, M. (2022). Feral fascists and deep green guerrillas: Infrastructural attack and accelerationist terror. *Critical Studies on Terrorism*, *15*(1), 169-208. https://doi.org/10.1080/17539153.2022.2031129. For examples of news media citing law enforcement sources, see: Wilson, C., & Ryan, J. (2023, January 19). *FBI warns of neo-Nazi plots as attacks on northwest power grid spike*. Oregon Public Broadcasting. Retrieved July 21, 2023, from https://www.opb.org/article/2023/01/19/surge-in-oregon-washington-substation-attacks-as-fbi-warns-neo-nazi-plots/; Sganga, N. (2023, February 17). *DHS "very concerned" about white nationalist attacks on power grid*. CBS News. Retrieved July 21, 2023, from https://www.cbsnews.com/news/dhs-white-nationalist-attacks-power-grid/; Lambert, E. (2023, April 24). *DHS warns tactics shared online threaten electrical grid*. NewsNation. Retrieved July 21, 2023, from https://www.newsnationnow.com/us-news/infrastructure/dhs-warning-online-tactics-electrical-grid-threats/

38 Jones, S. G., Doxsee, C., & Harrington, N. (2020). *The tactics and targets of domestic terrorists*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200729_Jones_TacticsandTargets_v4_FINAL.pdf; Jones, S. G., Doxsee, C., Harrington, N., Hwang, G., & Suber, J. (2020). *The war comes home: The evolution of domestic terrorism in the United States*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201021_Jones_War_Comes_Home_v2.pdf; Jones, S. G., Doxsee, C., Hwang, G., & Thompson, J. (2021). *The military, police, and the rise of terrorism in the United States*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210412_Jones_Military_Police_Rise_of_Terrorism_United_States_1.pdf?VersionId=_7p2zEfdFSVV5Vsva6bMlyp6I5MeXVL7; Doxsee, C., Jones, S. G., Thompson, J., Hwang, G., & Halstead, K. (2022). *Pushed to extremes: Domestic terrorism amid polarization and protest*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220517_Doxsee_PushedtoExtremes_DomesticTerrorism_0.pdf?VersionId=SdmZXk20Ymr7YNuRz3_hHVqMpyfbcM2t

39 Holt, T. J., Chermak, S. M., Freilich, J. D., Turner, N., & Greene-Colozzi, E. (2022). Introducing and exploring the Extremist Cybercrime Database (ECCD). Crime & Delinquency, 69(12). https://doi.org/10.1177/00111287221083899

40 This definition is informed by: Kriner, M. (2022, May 9). *An introduction to militant Accelerationism*. Accelerationism Research Consortium. Retrieved July 25, 2023, from https://www.accresearch.org/shortanalysis/an-introduction-to-militant-accelerationism; Miller, C. (2020, June 23). *'There is no political solution': Accelerationism in the white power movement*. Southern Poverty Law Center. https://www.splcenter.org/hatewatch/2020/06/23/there-no-political-solution-accelerationism-white-power-movement; Anti-Defamation League. (2019, April 16). White supremacists embrace "Accelerationism." https://www.adl.org/resources/blog/white-supremacists-embrace-accelerationism

41 Kriner, M., & Lewis, J. (2021). The evolution of the Boogaloo movement. *CTC Sentinel*, *14*(2), 22-32. https://ctc.westpoint.edu/wp-content/uploads/2021/02/CTC-SENTINEL-022021.pdf; Loadenthal, M. (2021, February 15). *Infrastructure, sabotage, and Accelerationism*. Global Network on Extremism & Technology. Retrieved July 21, 2023, from https://gnet-research.org/2021/02/15/infrastructure-sabotage-and-accelerationism/; Topor, L. (2019). Dark hatred: Antisemitism on the dark web. *Journal of Contemporary Antisemitism*, *2*(2), 25-42. https://doi.org/10.26613/jca/2.2.31; Fürstenberg, M. (2022). *Communities of hateful practice: The collective learning of accelerationist right-wing extremists with a case study of the Halle synagogue attack* (210). Max Planck Institute for Social Anthropology. https://pure.mpg.de/rest/items/item_3478774/component/file_3478775/content

42 DeBeck, C. (2019, July 22). *The dark web market is moving toward IaaS and MaaS – Here's why*. Security Intelligence. Retrieved July 21, 2023, from https://securityintelligence.com/posts/the-dark-web-market-is-moving-toward-iaas-and-maas-heres-why/. Also see: Montalbano, E. (2022, May 13). *Threat actors use Telegram to spread 'Eternity' Malware-as-a-Service*. Threatpost. Retrieved July 21, 2023, from https://threatpost.com/telegram-spread-eternity-maas/179623/; Marian, M. (2022, October 7). *LilithBot: New Malware-as-a-Service made available on Telegram*. Heimdal. Retrieved July 21, 2023, from https://heimdalsecurity.com/blog/lilithbot-new-malware-as-a-service-made-available-on-telegram; Mladenovska, M. (2023, January 9). *Understanding Malware-as-a-Service (MaaS): The future of cyber attack accessibility*. AT&T Cybersecurity. Retrieved July 21, 2023, from https://cybersecurity.att.com/blogs/security-essentials/understanding-malware-as-a-service-maas-the-future-of-cyber-attack-accessibility

43 Fritsch, L., Jaber, A., & Yazidi, A. (2023). *An overview of artificial intelligence used in malware*. In E. Zouganeli, A. Yazidi, G. Mello, & P. Lind (Eds.), *Nordic artificial intelligence research and development: 4th symposium of the Norwegian AI society, NAIS 2022, Oslo, Norway, May 31 – June 1, 2022, revised selected papers* (pp. 41-51). Springer Nature. https://doi.org/10.1007/978-3-031-17030-0_4

44 Korten, T. (2023, June 25). Latest threat to the electricity grid: White supremacists. *Sierra*. https://www.sierraclub.org/sierra/2023-2-summer/notes-here-there/latest-threat-electricity-grid-white-supremacists. Nevertheless, it remains an open question as to whether or not far-right extremists would be willing to kill transmission grid personnel if actors were in a situation where they felt it necessary to maintain operational security or continuity of plans, such as being identified while engaging in pre-attack surveillance or a worker being unexpectedly present at a site while an attack is imminent, respectively.

45 For an illustrative case of known potential insider threats within other parts of the energy sector, see: Nobel, J. (2021, July 21). *Whose allegiance? Three Percenters militia working in Bakken oil patch raises concerns of domestic terrorism risk*. DeSmog. Retrieved July 21, 2023, from https://www.desmog.com/2020/07/21/three-percenters-militia-bakken-oil-oneok-domestic-terrorism/; Price, L., & Prudente, T. (2021, January 7). Woman fatally shot during riot at U.S. Capitol formerly lived in Annapolis, worked at Calvert Cliffs. Baltimore Sun. Retrieved October 16, 2023, from https://archive.vn/JH7QS; Morlin, B. (1996, October 27). Terror suspect a nuclear expert kept low profile until arrest in valley blasts. Spokesman Review. Retrieved October 16, 2023, from https://www.spokesman.com/stories/1996/oct/27/terror-suspect-a-nuclear-expert-kept-low-profile/

46 For example, see: Beam, L. (1983). *Leaderless resistance*. Louisbeam.com. https://web.archive.org/web/20020924104229/www.louisbeam.com/leaderless.htm; Hoskins, R. K. (1997). *Vigilantes of Christendom: The story of the Phineas priesthood* (2nd ed.). The Virginia Publishing Company. https://ia601006.us.archive.org/29/items/312626264HoskinsRichardKellyVigilantesOfChristendom/312626264-Hoskins-Richard-Kelly-Vigilantes-of-Christendom.pdf

47 Emphasis on "intended." In practice, however, empirical evidence from multiple studies has suggested that many lone-actor terrorists have engaged in poor operational tradecraft, including operational security, manifesting "leakage" behaviors that allow law enforcement to identify and interdict plots. For a systematic review and summation of extant evidence on lone-actor terrorists, see: Kenyon, J., Baker-Beall, C., & Binder, J. (2021). Lone-actor terrorism – A systematic literature review. *Studies in Conflict & Terrorism*, *46*(10), 2038-65. https://doi.org/10.1080/1057610x.2021.1892635

48 Kenyon, J., Baker-Beall, C., & Binder, J. (2021). Lone-actor terrorism – A systematic literature review. *Studies in Conflict & Terrorism*, *46*(10), 2038-65. https://doi.org/10.1080/1057610x.2021.1892635

49 Clifford, B., & Melagrou-Hitchens, A. (2022). *Imitators or innovators? Comparing Salafi-jihadist and white supremacist attack planning in the United States*. Program on Extremism at George Washington University and NCITE. https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/Imitators-or-Innovators_Clifford-Meleagrou-Hitchens_NCITE_04212022.pdf

50 Krill, I., & Clifford, B. (2022). *Mayhem, murder, and misdirection: Violent extremist attack plots against critical infrastructure in the United States, 2016-2022*. Program on Extremism at George Washington University and NCITE. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/CriticalInfrastructureTargeting09072022.pdf

51 Bunker, R. J. (2022, December 29). *Weaponized aerial drones and the homeland: Increasing domestic terrorism concerns*. Homeland Security Today. Retrieved July 21, 2023, from https://www.hstoday.us/featured/weaponized-aerial-drones-and-the-homeland-increasing-domestic-terrorism-concerns/; ActionNewsJax.com News Staff. (2022, November 3). *Man behind certain antisemitic messaging in Jacksonville speaks out*. 104.5 WOKV. https://www.wokv.com/news/local/man-behind-certain-antisemitic-messaging-jacksonville-speaks-out/QQQOMGZ77NEG5PSPGYAK2CMERU/. Also see: Veilleux-Lepage, Y., Daymon, C., & Archambault, E. (2022). *Learning from foes: How racially and ethnically motivated violent extremists embrace and mimic the Islamic State's use of emerging technologies*. Global Network on Extremism & Technology. https://gnet-research.org/wp-content/uploads/2022/05/GNET-Report-Learning-From-Foes.pdf

52 This point bears further explanation and emphasis. Until recently, some analysts have noted that one of the major factors limiting far-right extremists' ability to experiment with aerial drone weaponization development has been the lack of a state-like support infrastructure. The conflict in Ukraine appears to be an opportunity for far-right extremists to overcome this barrier, as both nation-states involved in the conflict have provided their support to and infrastructure for far-right extremists willing to participate in the war. On general involvement and state support of far-right actors on both sides of the conflict, see, for example: Golinkin, L. (2023, June 13). *The Western media is whitewashing the Azov battalion*. The Nation. https://www.thenation.com/article/world/azov-battalion-neo-nazi/; Makuch, B. (2023, July 8). *Russian militia has links to American neo-Nazi and anti-trans figures*. The Intercept. https://theintercept.com/2023/07/08/american-neo-nazis-ukraine-war/. On far-right extremists and aerial drone weaponization, see: Haugstvedt, H. (2021). The right's time to fly? *The RUSI Journal*, *166*(1), 22-31. https://doi.org/10.1080/03071847.2021.1906161. On innovation of aerial drone weaponization resulting from nonstate involvement in Ukraine, broadly, see: Haugstvedt, H. (2023). A flying reign of terror? The who, where, when, what, and how of nonstate actors and armed drones. *Journal of Human Security*, *19*(1). https://doi.org/10.12924/johs2023.19010001. On specific far-right extremist aerial drone innovation resulting from involvement in the Ukraine conflict, see: Stalinsky, S., Smith, A., Sosnow, R., Agron, A., Purdue, S., Dressler, R., & Wolfson, A. (2023, May 18). *Neo-Nazi, white supremacist, and anti-government groups in the U.S. and around the world embrace drones for combat, spreading ideology and harassing minorities – 2021-2023*. Middle East Media Research Institute. Retrieved July 21, 2023, from https://www.memri.org/dttm/neo-nazi-white-supremacist-and-anti-government-groups-us-and-around-world-embrace-drones-combat

53 Havard Haugstevdt, who has published research on far-right extremists' weaponized use of aerial drones, points out that knowledge of 3D printing has previously helped other violent extremists, like operatives associated with the Islamic State of Iraq and Syria, construct parts of an aerial drone or their weapons components. Citing cases associated with ISIS operatives, he notes, "Research conducted on the actions of such groups has revealed evidence of 3D printing of some parts of the UAV itself, or parts fitted to the explosive being dropped from the UAV [unnamed aerial vehicle {i.e. an aerial drone}]." Evidence from previous arrests and terrorist attacks indicates significant interest among far-right extremists in utilizing 3D printing technology. Thus far, their embrace of the technology appears to be almost entirely centered on the development and manufacturing of firearms. However, there is no reason to think this cannot change, especially given the fertile learning and innovation environment provided by the Ukraine-Russia conflict. Not only has the conflict provided far rightists an opportunity to gain valuable direct combat experience that could provide operationally useful skills to enact a terrorist attack, the conflict has also made extensive weaponized use of commercial drones, bomb making, 3D printing technology, and their intersections. On far-right extremists and aerial drones, see: Haugstvedt, H. (2021). The right's time to fly? *The RUSI Journal*, *166*(1), 22-31. https://doi.org/10.1080/03071847.2021.1906161. On far-right extremists and 3D-printed firearms, see: Basra, R. (2022, June 23). *The future is now: The use of 3D-printed guns by extremists and terrorists*. Global Network on Extremism & Terrorism. https://gnet-research.org/2022/06/23/the-future-is-now-the-use-of-3d-printed-guns-by-extremists-and-terrorists/. On commercial drones and 3D printing in the Ukraine conflict, see: Sachedina, O., & Bogart, N. (2022, May 4). *How drones and 3D-printed weapon technology are revolutionizing the battlefield in Ukraine*. CTVNews. Retrieved September 18, 2023, from https://www.ctvnews.ca/world/how-drones-and-3d-printed-weapon-technology-are-revolutionizing-the-battlefield-in-ukraine-1.5889326; Feldman, A. (2022, May 31). *Putting 3D printers to work in Ukraine's war zone*. Forbes. https://www.forbes.com/sites/amyfeldman/2022/03/31/putting-3d-printers-to-work-in-ukraines-war-zone/?sh=58b2453a5015; Baker, S. (2023, August 2). *Ukraine is 3D printing bombs to keep up with its battlefield demands, says report, with some costing as little as $3.85*. Business Insider. https://www.businessinsider.com/ukraine-3d-printing-bombs-drop-on-russia-soldiers-battlefield-report-2023-8?op=1; Khurshudyan, I., & Hrabchuk, K. (2023, April 8). *Facing critical ammunition shortage, Ukrainian troops ration shells*. The Washington Post. https://archive.vn/exF07

54 Veilleux-Lepage, Y., Daymon, C., & Archambault, E. (2022). *Learning from foes: How racially and ethnically motivated violent extremists embrace and mimic the Islamic State's use of emerging technologies*. Global Network on Extremism & Technology. https://gnet-research.org/wp-content/uploads/2022/05/GNET-Report-Learning-From-Foes.pdf, p. 22.

55 Criezis, M. (2020). Intersections of extremisms: White nationalist/Salafi-Jihadi propaganda overlaps and essentialist narratives about Muslims. *Journal of Education in Muslim Societies*, *2*(1). https://doi.org/10.2979/jems.2.1.06

56 As Nina Silove points out in her incisive review on conceptualizations of "grand strategy," among academic scholars, it has taken on "three distinct meanings. First, scholars use grand strategy to refer to a deliberate, detailed plan devised by individuals. Second, they employ it to refer to an organizing principle [or set of principles] that is consciously held and used by individuals to guide their decisions. Third, scholars use the term to refer to a pattern in state behavior." In the context of this publication, the authors' reference to grand strategy is within this second meaning, as a set of guiding principles to guide the actions of individuals – in this case, nonstate violent extremists. See: Silove, N. (2018). Beyond the buzzword: The three meanings of "grand strategy." *Security Studies*, *27*(1), 27-57. https://doi.org/10.1080/09636412.2017.1360073

57 Here the prefix "inclusive" is added, because there are some white nationalists who do advocate for a type of exclusionary multiculturalism, perhaps most famously articulated in far-right ideologue Alain de Benoist's concept of "ethnopluralism." As Daniel Sueda, a scholar who published research on this topic, summarizes, "de Benoist explains that he opposes the idea of racial superiority (he rather thinks that every race has its own 'genius'), but also left-wing 'anti-racism', which for him acts as a homogenizing force that imposes western values on nonwhite peoples. He proposes, instead of cultural interbreeding, to guarantee the autonomy of every ethnie and build harmonious societies that avoid hate and prejudice through a respect for diversity." See: Rueda, D. (2021). Alain de Benoist, ethnopluralism and the cultural turn in racism. *Patterns of Prejudice*, *55*(3), 213-235. https://doi.org/10.1080/0031322x.2021.1920722

58 Fenton, J. (2023, February 6). *Woman plotted to destroy energy substations with neo-Nazi leader, FBI says*. The Baltimore Banner. Retrieved July 21, 2023, from https://www.thebaltimorebanner.com/community/criminal-justice/sarah-beth-clendaniel-fbi-energy-substation-plot-KLTNJHK3FNBG5JHT7THIR3GQAY/

59 Loadenthal, M. (2022). Feral fascists and deep green guerrillas: Infrastructural attack and accelerationist terror. *Critical Studies on Terrorism*, *15*(1), 169-208. https://doi.org/10.1080/17539153.2022.2031129

60 The clearest example of this was the March 15, 2019, terrorist attacks in Christchurch, New Zealand, by a white supremacist. On the attack, the perpetrator's manifesto, and its use of eco-fascism to justify the attacks, see: Beutel, A. J. (2019, April 30). *The New Zealand terrorist's manifesto: A look at some of the key narratives, beliefs and tropes*. START Center. https://www.start.umd.edu/news/new-zealand-terrorists-manifesto-look-some-key-narratives-beliefs-and-tropes

61 Thompson, J. (2021, June 30). Examining extremism: The Boogaloo movement. *Center for Strategic and International Studies*. https://www.csis.org/blogs/examining-extremism/examining-extremism-boogaloo-movement; Beutel, A., & Johnson, D. (2021, June 8). *The three percenters: A look inside an anti-government militia*. New Lines Institute for Strategy and Policy. https://newlinesinstitute.org/wp-content/uploads/20210225-Three-Percenter-PR-NISAP-rev051021.pdf

62 Thompson, J. (2021, June 30). Examining extremism: The Boogaloo movement. *Center for Strategic and International Studies*. https://www.csis.org/blogs/examining-extremism/examining-extremism-boogaloo-movement; Doxsee, C. (2021, August 12). Examining extremism: The militia movement. *Center for Strategic and International Studies*. https://www.csis.org/blogs/examining-extremism/examining-extremism-militia-movement

63 Sollenberger, R. (2021, February 27). *Talking to the boogaloo: An exclusive series of conversations with a would-be revolutionary*. Salon. Retrieved July 21, 2023, from https://www.salon.com/2021/02/27/talking-to-the-boogaloo-an-exclusive-series-of-conversations-with-a-would-be-revolutionary/; Doxsee, C. (2021, August 12). Examining extremism: The militia movement. *Center for Strategic and International Studies*. https://www.csis.org/blogs/examining-extremism/examining-extremism-militia-movement; Thompson, J. (2021, June 30). Examining extremism: The Boogaloo movement. *Center for Strategic and International Studies*. https://www.csis.org/blogs/examining-extremism/examining-extremism-boogaloo-movement

64 Kriner, M., Newhouse, A., & Lewis, J. (2021, November 18). *Understanding Accelerationist narratives: The Boogaloo*. Global Network on Extremism & Technology. https://gnet-research.org/2021/11/18/understanding-accelerationist-narratives-the-boogaloo/

65 START. (n.d.). *Global Terrorism Database search results*. START.umd.edu. Retrieved September 18, 2023, from https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=197004130001

66 For example, see: Fireant Collective. (2001, May). Setting fires with electrical timers: An Earth Liberation Front guide; Foreman, D. (1993, July). Eco-defense: A field manual to monkey wrenching. Abbzug Publishing.

67 For a comprehensive overview of these practices from a primary source, see: The Dam Collective. (2020). *Earth first! Direct action manual* (3rd ed.). https://web.archive.org/web/20210508014918/https://mutualaiddisasterrelief.org/wp-content/uploads/2021/04/direct_action_manual_3-1.pdf

68 Bunker, R. J. (2022, December 29). *Weaponized aerial drones and the homeland: Increasing domestic terrorism concerns*. Homeland Security Today. Retrieved July 21, 2023, from https://www.hstoday.us/featured/weaponized-aerial-drones-and-the-homeland-increasing-domestic-terrorism-concerns/

69 Miller, E. (2016). *Terrorist attacks targeting critical infrastructure in the United States, 1970-2015*. University of Maryland START Center. https://web.archive.org/web/20190430195710/https://www.start.umd.edu/pubs/DHS_I%26A_GTD_Targeting%20Critical%20Infrastructure%20in%20the%20US_June2016.pdf

70 On this point and in comparison with far-right extremists who co-opt environmental concerns, see: Loadenthal, M. (2017). "Eco-terrorism": An incident-driven history of attack (1973–2010). *Journal for the Study of Radicalism*, *11*(2), 1-34. https://doi.org/10.14321/jstudradi.11.2.0001; Loadenthal, M. (2022). Feral fascists and deep green guerrillas: Infrastructural attack and accelerationist terror. *Critical Studies on Terrorism*, *15*(1), 169-208. https://doi.org/10.1080/17539153.2022.2031129

71 For example, see: Anonymous Contributor. (2016, September 14). *Unbolting against the new Hydro-Quebec high-tension line*. It's Going Down. https://web.archive.org/web/20170208063317/https://itsgoingdown.org/unbolting-new-hydro-quebec-high-tension-line/

72 A particularly illustrative example was a prevented terrorist attack against a rail line carrying equipment to build a cross-border natural gas pipeline between Canada and the United States. The attack used "shunts" – devices that interfere with train signals and cause derailments – on the tracks and were allegedly carried out by two left-wing anarchists, Samantha Brooks and Ellen Brennan Reiche. Prior to the arrests, there were 41 similar incidents involving railway sabotage, several of which used shunts, close to the area where Brooks and Reiche placed their devices. See: Beaumont, H. (2021, July 29). *The activists sabotaging railways in solidarity with Indigenous people*. The Guardian. https://www.theguardian.com/environment/2021/jul/29/activists-sabotaging-railways-indigenous-people; Anonymous Contributor. (2020, January 22). *Whatcom County, WA: Rail shut down in solidarity with the Wet'suwet'en fight against colonial invasion*. It's Going Down. https://itsgoingdown.org/whatcom-county-wa-rail-shut-down-in-solidarity-with-the-wetsuweten-fight-against-colonial-invasion/

73 Anonymous Contributor. (2016, September 14). *Unbolting against the new Hydro-Quebec high-tension line*. It's Going Down. https://web.archive.org/web/20170208063317/https://itsgoingdown.org/unbolting-new-hydro-quebec-high-tension-line/

74 Holt, T. J., Stonhouse, M., Freilich, J., & Chermak, S. M. (2019). Examining ideologically motivated cyberattacks performed by far-left groups. *Terrorism and Political Violence*, *33*(3), 527-548. https://doi.org/10.1080/09546553.2018.1551213; Holt, T. J., Chermak, S. M., Freilich, J. D., Turner, N., & Greene-Colozzi, E. (2022). Introducing and Exploring the Extremist Cybercrime Database (ECCD). Crime & Delinquency, 69(12), 2411-36. https://doi.org/10.1177/00111287221083899

75 Hamill, J. (2017, January 27). *Anonymous hacktivists publish guide on how to HACK Donald Trump's smartphone*. The Sun. https://www.thesun.co.uk/news/2723459/anonymous-hacktivists-publish-guide-on-how-to-hack-donald-trumps-smartphone/

76 Sharma, A. (2021, September 15). *Anonymous leaks gigabytes of data from alt-right web host Epik*. Ars Technica. https://arstechnica.com/information-technology/2021/09/anonymous-leaks-gigabytes-of-data-from-epik-web-host-of-gab-and-parler/

77 Holt, T. J., Stonhouse, M., Freilich, J., & Chermak, S. M. (2019). Examining ideologically motivated cyberattacks performed by far-left groups. *Terrorism and Political Violence*, *33*(3), 527-548.

78 Loadenthal, M. (2017). "eco-terrorism": An incident-driven history of attack (1973–2010). *Journal for the Study of Radicalism*, *11*(2), 1-34. https://doi.org/10.14321/jstudradi.11.2.0001; Copsey, N., & Merrill, S. (2020). Violence and restraint within Antifa: A view from the United States. Perspectives on Terrorism, 14(6), 122–138. https://www.jstor.org/stable/26964730; Busher, J., Holbrook, D., & Macklin, G. (2021). How the "internal brakes" on violent escalation work and fail: Toward a conceptual framework for understanding intra-group processes of restraint in militant groups. *Studies in Conflict & Terrorism*, 46(10), 1960-83. https://doi.org/10.1080/1057610x.2021.1872156; Busher, J., Holbrook, D., & Macklin, G. (2019). The internal brakes on violent escalation: A typology. *Behavioral Sciences of Terrorism and Political Aggression*, *11*(1), 3-25. https://doi.org/10.1080/19434472.2018.1551918

79 Knake, R. K. (2017). *A cyberattack on the U.S. power grid* (Contingency Planning Memorandum No. 31). Council on Foreign Relations. https://cdn.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf

80 Violent animal rights extremists and eco-terrorists primarily engage in property destruction. They have yet to show a willingness to actively kill, or otherwise seriously harm, human beings. However, there have been aspirational online discussions about the merits of killing people on behalf of these causes on animal rights and environmental extremists message boards, chatrooms, and elsewhere. For an illustrative case, see: Heller, J. (2013, January 16). *Arson, cracked testicles, and Internet death threats: How animal rights extremists are learning from the people who murdered George Tiller*. Gawker. Retrieved July 21, 2023, from https://www.gawker.com/5976473/arson-cracked-testicles-and-internet-death-threats-how-animal-rights-extremists-are-learning-from-the-people-who-murdered-george-tiller

81 The example of animal rights extremist Camille Marino provides at least partial support for this scenario. Marino had previously worked as an investment banker, which may not necessarily be a job occupation opposed to animal rights, per se, but is not one that would be easily associated with it, either, given the left-leaning and often capitalist-skeptical milieu of animal rights activism. While working as an investment banker, according to one news account of her life and extremist activism, she had read articles on the mistreatment of animals commonly associated with factory farming practices. As a result, "she immediately became a vegan and was shortly thereafter radicalized in her thinking." However, it is unclear if she had maintained her pro-capitalist job occupation for any period of time after she began embracing extremist beliefs. The larger point here is many different people from many different walks of life can end up embracing ideas and belief systems that at first glance may seem at odds with their backgrounds. Heller, J. (2013, January 16). *Arson, cracked testicles, and Internet death threats: How animal rights extremists are learning from the people who murdered George Tiller*. Gawker. Retrieved July 21, 2023, from https://www.gawker.com/5976473/arson-cracked-testicles-and-internet-death-threats-how-animal-rights-extremists-are-learning-from-the-people-who-murdered-george-tiller

82 Anti-Defamation League. (2005, February 5). *Ecoterrorism: Extremism in the animal rights and environmentalist movements*. https://www.adl.org/resources/report/ecoterrorism-extremism-animal-rights-and-environmentalist-movements; Barboe, J. F. (2002, February 12). *The threat of eco-terrorism*. Federal Bureau of Investigation. https://archives.fbi.gov/archives/news/testimony/the-threat-of-eco-terrorism; Chermak, S. M., Freilich, J., Duran, C., & Parkin, W. S. (2013). *An overview of bombing and arson attacks by environmental and animal rights extremists in the United States, 1995-2010: Final report to the Resilient Systems Division, Science and Technology Directorate, U.S. Department of Homeland Security*. University of Maryland START Center. https://www.dhs.gov/sites/default/files/publications/OPSR_TP_TEVUS_Bombing-Arson-Attacks_Environmental-Animal%20Rights-Extremists_1309-508.pdf

83 START. (2023, July 21). *Global Terrorism Database search results*. START.umd.edu. Retrieved July 21, 2023, from https://www.start.umd.edu/gtd/search/Results.aspx?page=1&casualties_type=b&casualties_max=&dtp2=all&country=217&target=21&count=100&charttype=line&chart=overtime&ob=GTDID&od=desc&expanded=yes#results-table. The results are all attacks against public utilities in the United States documented by the GTD since 1970.

84 START. (2023, July 21). *Global Terrorism Database search results*. START.umd.edu. Retrieved July 21, 2023, from https://www.start.umd.edu/gtd/search/Results.aspx?page=1&casualties_type=b&casualties_max=&dtp2=all&country=217&target=21&count=100&charttype=line&chart=overtime&ob=GTDID&od=desc&expanded=yes#results-table. The results are all attacks against public utilities in the United States documented by the GTD since 1970.

85 Deshpande, N., & Ernst, H. (2012). *Countering eco-terrorism in the United States: The case of 'Operation Backfire.' Final report to the Science & Technology Directorate, U.S. Department of Homeland Security*. https://www.start.umd.edu/pubs/START_EffectivenessofLECountermeasuresOperationBackfire_Sept2012.pdf; START. (n.d.). *Incident summary for GTDID: 199912300002*. Retrieved July 21, 2023, from https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=199912300002

86 For example, see: US v. Konopka, 409 F.3d 837 (7th Cir. 2005) https://law.justia.com/cases/federal/appellate-courts/F3/409/837/561522/, noting, "Between 1997 and 2001, Joseph Konopka, alias Dr. Chaos, a self-styled supervillain, together with accomplices (some recruited from the Web site 'Teens for Satan'), committed a series of criminal acts apparently just for the hell of it—acts such as destroying electrical and telecommunications facilities, disabling airline navigation systems, setting fire to buildings, intercepting electronic communications, and trafficking in counterfeit goods" (emphasis added). In a 2020 interview with local Chicago news outlet WGN, Konopka later claimed that his actions were not motived by "anti-authority" feelings, but simply the rash decisions of a young man. One should be skeptical of Konopka's claim, given that, in addition to his explicit lack of remorse for past actions, several of his and his associates' targets were not merely specific individuals, but entire communities and entities that are symbols of government authority and service provision, including the Wisconsin Air National Guard, Wisconsin Public Radio, and at least 28 electrical service providers, causing interruptions affecting over 30,000 customers. See: Donlon, J. (2019, November 18). *WGN investigates Dr. Chaos – a 4-part podcast and TV series 'Chasing chaos.'* WGN-TV. https://wgntv.com/news/wgn-investigates/wgn-investigates-chasing-chaos/; Associated Press. (n.d.). *'Dr. Chaos' indicted in Wisconsin utility attacks*. SecLists.Org Security Mailing List Archive. https://seclists.org/isn/2002/May/45; Hamill, S. D.,

Heinzmann, D., & Walberg, M. (2002, March 13). *Computer whiz to 'Dr. Chaos.'* Chicago Tribune. https://www.chicagotribune.com/news/ct-xpm-2002-03-13-0203130362-story.html; Held, T. (2002, March 14). *Judge calls 'Dr. Chaos' a true danger*. Milwaukee Journal Sentinel. https://web.archive.org/web/20071102143747/http://www.jsonline.com/story/index.aspx?id=27073; Imrie, R. (2002, March 12). *Family of man with cyanide responds*. Midland Reporter-Telegram. https://www.mrt.com/news/article/Family-of-Man-With-Cyanide-Responds-7832431.php; Barton, G. (2002, May 7). *Prosecutors say crime spree wreaked havoc*. Milwaukee Journal Sentinel. https://seclists.org/isn/2002/May/64

87 Associated Press. (2003, November 20). *Man pleads guilty to power line sabotage*. Herald and News. https://www.heraldandnews.com/news/top_stories/man-pleads-guilty-to-power-line-sabotage/article_b0156ae0-3e79-5092-8c2a-694a9fc52351.html; Associated Press. (2003, November 3). Wanted man in custody. *Redding Record Searchlight*, pp. A1, A5.

88 United Press International. (2002, May 8). *Wisconsin's 'Dr. Chaos' indicted*. https://www.upi.com/Archives/2002/05/08/Wisconsins-Dr-Chaos-indicted/3211020830400/

89 WGN9 (2020, April 6). "'Dr. Chaos' back in court."

90 McCormick, J., & Tribune staff reporter (2003, March 14). Man who hid cyanide in CTA tunnel sentenced. Chicago Tribune. https://www.chicagotribune.com/news/ct-xpm-2003-03-14-0303140293-story.html

91 Seidel, J. (2020, April 3). *Nearly two decades after cyanide scare, feds keeping close eye on 'Dr. Chaos.'* Chicago Sun-Times. https://chicago.suntimes.com/2020/4/3/21207392/dr-chaos-cyanide-feds-keep-close-eye

92 Pagliery, J. (2015, October 17). *Sniper attack on California power grid may have been 'an insider,' DHS says*. CNN. Retrieved July 21, 2023, from https://money.cnn.com/2015/10/16/technology/sniper-power-grid/index.html; Salahieh, N., & Sarisohn, H. (2022, December 5). *Tens of thousands still in the dark after 'targeted' attacks on North Carolina power substations*. CNN. https://www.cnn.com/2022/12/05/us/power-outage-moore-county-investigation-monday/index.html; Bergengruen, V. (2023, January 9). *Authorities fear extremists are targeting U.S. power grid*. Time Magazine. https://time.com/6244977/us-power-grid-attacks-extremism/

93 Johnson, D., & Beutel, A. J. (2022). *Protecting the U.S. government from far-right insider threats*. New Lines Institute for Strategy and Policy. https://newlinesinstitute.org/wp-content/uploads/20220928-Protect-US-from-Far-Right-NLISAP.pdf

94 ICF International. (2016). *Electric grid security and resilience: Establishing a baseline for adversarial threats*. https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf

95 National Infrastructure Advisory Council. (2008). *Insider threat to critical infrastructures: Final report and recommendations*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/niac-insider-threat-final-report-04-08-08-508.pdf

96 Thalen, M. (2023, January 21). *Exclusive: U.S. airline accidentally exposes 'No Fly List' on unsecured server*. The Daily Dot. https://www.dailydot.com/debug/no-fly-list-us-tsa-unprotected-server-commuteair/; Warikoo, N. (2019, September 9). *Michigan Muslims hope judge's ruling against terror watch list ends harassment by feds*. Detroit Free Press. Retrieved July 24, 2023, from https://www.freep.com/story/news/local/michigan/2019/09/09/judge-terrorism-watch-list-violates-civil-rights-muslims/2217731001/; Barakat, M. (2019, February 20). *APNewsBreak: Feds share watchlist with 1,400 private groups*. AP News. Retrieved July 24, 2023, from https://apnews.com/article/ae4779a057c04947a332fce64f6cf345.

97 Barrett, D., Hsu, S. S., & Lang, M. J. (2021, January 14). *Dozens of people on FBI terrorist watch list came to D.C. the day of Capitol riot*. Washington Post. https://archive.vn/c0XWU

98 For example, see: Bell, A. J., Rogers, M. B., & Pearce, J. M. (2019). The insider threat: Behavioral indicators and factors influencing likelihood of intervention. *International Journal of Critical Infrastructure Protection*, *24*, 166-176. https://doi.org/10.1016/j.ijcip.2018.12.001

99 The recommendation for behavioral observation practices within a larger insider threat/risk mitigation program does not come without caution. If not run carefully, they can also engage in unwarranted surveillance and bias against employees. See: Schwellenbach, N. (2022, December 12). *Hundreds of Oath Keepers have worked for DHS, leaked list shows*. Project On Government Oversight. Retrieved July 24, 2023, from https://www.pogo.org/investigation/2022/12/hundreds-of-oath-keepers-have-worked-for-dhs-leaked-list-shows. For an example of behavioral observation malfunction, see: Ackerman, S. (2017, March 22). *Muslims inside FBI describe culture of suspicion and fear: 'It is cancer.'* The Guardian. https://www.theguardian.com/us-news/2017/mar/22/fbi-muslim-employees-discrimination-religion-middle-east-travel. For an example of behavioral observation success, see: Defense Counterintelligence and Security Agency. (n.d.). Case study: Kinetic violence -- A positive outcome. Center for Development of Security Excellence. https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-paul-hasson.pdf, noting, "Christopher Paul Hasson [a violent white supremacist extremist] was arrested on February 15, 2019, which prevented him from possibly carrying out acts of violence. His arrest followed a multi-year investigation that included monitoring the use of his U.S. Government automated information system" (emphasis added).

100 Smith, A. (2020, August 4). *Employees may be fired for hate speech on social media*. SHRM. Retrieved July 21, 2023, from https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/employees-fired-for-hate-speech-on-social-media.aspx

101 CERT Insider Threat Center. (2016). *Common sense guide to mitigating insider threats, fifth edition* (CMU/SEI-2015-TR-010). Carnegie Mellon University Software Engineering Institute. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

102 Bunn, M., & Sagan, S. D. (2014). *A worst practices guide to insider threats: Lessons from past mistakes*. American Academy of Arts and Sciences. https://www.amacad.org/sites/default/files/publication/downloads/insiderThreats.pdf

103 Glass, E., & Glass, V. (2018). We are one terrorist attack away from a major nationwide blackout: What should we do? *Rutgers Business Review*, *3*(2), 144-158. https://rbr.business.rutgers.edu/sites/default/files/documents/rbr-030204.pdf

104 See: Shook, T. (2022, December 5). *Moore County substation attacks: 35K still without power as temperatures drop*. The Fayetteville Observer. https://www.fayobserver.com/story/news/2022/12/05/moore-county-nc-updates-more-than-35k-residents-still-without-power/69701437007/. Although the attackers and their underlying motives have not been officially confirmed, according to one news report shortly after the incident, "investigators...are zeroing in on two threads of possible motives centered around extremist behavior for the weekend assault on two North Carolina electric substations, according to law-enforcement [sic.] sources briefed on the investigation." See: Miller, J., Almasy, S., & Wild, W. (2022, December 8). *Investigators are zeroing in on two possible motives centered around extremist behavior in NC power stations attacks, sources say*. CNN. https://www.cnn.com/2022/12/07/us/power-outage-moore-county-investigation-wednesday/index.html

105 A noteworthy example of research positively moving in this direction was a 2022 report on violent extremist attacks against U.S. critical infrastructure co-published by the George Washington University Program on Extremism (POE) and the University of Nebraska-Omaha's National Counterterrorism Innovation, Technology, and Education Center (NCITE). Despite the imagery on the cover page, the POE-NCITE report dealt with "critical infrastructure" broadly, not the transmission grid, specifically. Moreover, it was limited by its focus on violent jihadist extremists and violent white supremacist extremists, leaving out analysis of other prominent actors like far-right militia extremists and far leftists. See: Krill, I., & Clifford, B. (2022). *Mayhem, murder, and misdirection: Violent extremist attack plots against critical infrastructure in the United States, 2016-2022*. Program on Extremism at George Washington University and NCITE. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/CriticalInfrastructureTargeting09072022.pdf

106 For an illustrative example of this kind of research, see: Bell, A. J., Rogers, M. B., & Pearce, J. M. (2019). The insider threat: Behavioral indicators and factors influencing likelihood of intervention. *International Journal of Critical Infrastructure Protection*, *24*, 166-176. https://doi.org/10.1016/j.ijcip.2018.12.001

107 Various messages posted in "A Well Regulated Militia" forum during 2008, 2009, and 2010. Posts on file with author (Johnson).

Contact

For media inquiries, email media@newlinesinstitute.org

To submit a piece to the New Lines Institute, email submissions@newlinesinstitute.org

For other inquiries, send an email to info@newlinesinstitute.org

1776 Massachusetts Ave. N.W., Suite 120
Washington, D.C., 20036

(202) 800-7302

Connect With Us

@newlinesinst | @New Lines Institute for Strategy and Policy | Subscribe | Sign up

NEW LINES INSTITUTE
FOR STRATEGY AND POLICY