From Earth Liberation to Accelerationism: A High-Level Review of Fifty Years of Domestic Infrastructure Terrorism

By Jesse Humpal

This article reviews 50 years of domestic extremist attacks and plots against U.S. critical infrastructure and infrastructure-adjacent industrial and commercial targets. Using an original open-source dataset (1970–July 2025) compiled from terrorism incident databases, government reporting, and a systematic review of federal case records, it documents how sabotage has appeared across ideologically divergent milieus, with two dominant clusters: environmental and animal-rights extremism (peaking in the late 1990s and early 2000s) and a post-2015 rise in far-right extremist infrastructure plotting, including a subset of cases that explicitly reflect accelerationist intent. The analysis distinguishes between issue-driven eco-sabotage that frequently targets grievance-linked commercial and industrial nodes and more contemporary plots that more often privilege critical systems, particularly the electric grid, for cascading disruption. A decade-by-decade narrative traces tactical evolution from arson and clandestine cells to digitally networked mobilization, firearms, and higher-casualty-risk methods. The article concludes by assessing the evolution of law-enforcement and policy responses, including post-9/11 eco-terrorism prosecutions, infrastructure reliability and physical-security standards, and more recent use of energy-facility statutes and intelligence sharing with owners and operators.

In February 2023, U.S. authorities foiled a neo-Nazi plot to sabotage five electrical substations around Baltimore, Maryland, a scheme intended to "completely destroy" power to the predominantly Black city.[1] This far-right extremism accelerationist conspiracy, driven by racist ideology, echoes a very different wave of sabotage from 25 years earlier: On October 19, 1998, eco-extremists with the Earth Liberation Front (ELF) burned down part of the Vail Ski Resort in Colorado to protest its expansion into a lynx habitat, causing an estimated $12 million in damage.[2] Though the perpetrators' worldviews could not be further apart, these incidents underscore a striking convergence: Ideologically divergent extremist movements—from 1990s radical environmentalists to 2020s accelerationists—have fixated on U.S. critical and infrastructure-adjacent targets. In this article, 'accelerationism' refers to a strategic logic that treats violence as a means to hasten social breakdown and widen conflict, rather than a single ideology; while much contemporary infrastructure plotting emerges from far-right extremist milieus, accelerationist ideas can be adopted across ideologies. However, the data also shows a consistent targeting asymmetry: Eco-extremist campaigns more often focus on infrastructure-adjacent commercial and industrial sites linked to a specific grievance, while accelerationist actors more frequently privilege truly critical systems—especially the electric grid—for cascading disruption.

Open-source data shows that since the 1970s, domestic extremist ideologies have motivated a substantial number of attacks and plots against infrastructure in the United States. For example, between 1995 and 2010, the ELF and its sister group the Animal Liberation Front (ALF) orchestrated 239 arsons and bombings across the United States in the name of defending nature and animals.[3] By the early 2000s, the FBI estimated these eco-extremists had committed over 600 criminal acts (from vandalism to arson) causing more than US$43 million in damage between 1996 and 2002.[4] Fast forward to the late 2010s-2020s, and a new wave of extremist targeting has emerged: Research by the Program on Extremism at George Washington University found that 13 white supremacists were charged in federal court for planning attacks on the U.S. energy sector from 2016 to 2022.[5] The U.S. Department of Homeland Security (DHS) reports that physical attacks on the electric grid hit an all-time high in 2022, with 163 direct incidents, a 77 percent increase from the prior year.[6] These numbers include both criminal vandalism and extremist sabotage, but officials note a distinct rise in plots driven by racially or ethnically motivated violent extremists (REMVEs) this decade.

Despite their vastly different motives, these two extremes exhibit remarkable similarities in how and why they attack infrastructure.

Lieutenant Colonel Jesse R. Humpal, PhD, is an active-duty U.S. Air Force officer and an Assistant Professor of Political Science at the United States Air Force Academy. His research focuses on U.S. national security policy, with particular emphasis on critical infrastructure resilience, defense industrial policy, extremism, and the strategic implications of national security spending. He previously served as Director for Resilience on the National Security Council staff, where he led interagency efforts on Position, Navigation, and Timing (PNT) policy, National Security Memorandum implementation, and critical infrastructure security. His writing has appeared in outlets and journals including War on the Rocks, Lawfare, Joint Force Quarterly, Foreign Policy, Newsweek, The Washington Post, *and the* Journal of Critical Infrastructure Policy.

The views expressed are solely those of the author and do not reflect the official policy or position of the U.S. Air Force, the U.S. Air Force Academy, the Department of War, or the U.S. Government.

Both frame their crimes as urgent direct action against an intolerable status quo, but for eco-saboteurs that status quo is often a specific practice or project they want to halt, whereas for accelerationists it is a tyrannical government and the multicultural society it protects, which they seek to collapse and replace. And as the name of the ELF's 2001 communiqué "Setting Fires for Effect" suggested, both extremes believe that striking critical nodes (power grids, pipelines, railways) will send a powerful symbolic message and precipitate broader chaos or reform.[7] These commonalities, and the evolution in tactics from one era to the next, carry important implications for counterterrorism policy, infrastructure security, and resource allocation against domestic violent extremists (DVEs) of all stripes. Online ecosystems have increasingly facilitated limited cross-ideological borrowing, with tactics, manuals, and propaganda circulating across extremist milieus.

This article presents a data-driven analysis of U.S. extremist sabotage against critical and infrastructure-adjacent targets from the 1970s through mid-2025. It begins with a comprehensive quantitative overview of documented attacks and plots against the nation's energy, transportation, communication, and water infrastructure by both left-wing and right-wing extremists. This section establishes the scale and scope of the threat and identifies key patterns across time, geography, and ideology.

The article then turns to a decade-by-decade examination, tracing the evolution of tactics and motivations. It explores the early environmental and animal-rights campaigns of the ALF and ELF during the 1990s, such as the 1998 Vail arson and the subsequent FBI Operation Backfire crackdown, and follows the transition to more contemporary attacks and plots, including the 2022 Moore County, North Carolina, substation attack and the foiled 2023 Baltimore plot.

A comparative analysis follows, contrasting how violent far-left and violent far-right extremist movements differ in their motives, targets, tactics, organizational structures, and communications while highlighting points of convergence—most notably their shared "accelerationist" logic and the cross-pollination of sabotage tactics across ideological lines.

Finally, the article examines the evolution of law enforcement and policy responses, from the post-9/11 focus on eco-terrorism under Operation Backfire and the Animal Enterprise Terrorism Act (AETA) to more recent DHS and FBI warnings about domestic violent extremist threats to the U.S. energy sector. This section also compares prosecution patterns and sentencing outcomes under statutes such as 18 U.S.C. § 1366 (destruction of an energy facility) and terrorism enhancements, illustrating how federal agencies have adapted in responding to shifting threat landscapes.

Data Compilation: Incidents, Targets, and Trends (1970-mid-2025)

Scope and Sources

This article distinguishes between critical infrastructure (as defined by CISA sectors) and infrastructure-adjacent industrial and commercial targets—assets that enable, support, or symbolize industrial activity but whose disruption would not necessarily meet the threshold for 'critical' under federal definitions.[a] The dataset compiles extremist-motivated attacks and plots against such infrastructure on U.S. soil from 1970 through mid-2025. It draws on open sources including the START Global Terrorism Database (GTD), the CSIS U.S. Terrorism Incidents database, the U.S. Department of Energy's OE-417 electric-disturbance reports, U.S. Department of Justice/FBI press releases, and the George Washington University Program on Extremism's Domestic Extremism tracker.[8] Both completed attacks and foiled plots are included, provided ideological motivation is evidenced. Foiled plots were identified primarily through federal indictments, criminal complaints, plea agreements, and sentencing memoranda, supplemented by DOJ and FBI press releases, allowing for systematic coverage of disrupted plots across the full study period. Each incident was coded for date, location, target type, perpetrator affiliation, ideology, method (bombing, arson, firearm attack, cyber), casualties (if any), outcome, and source reference.

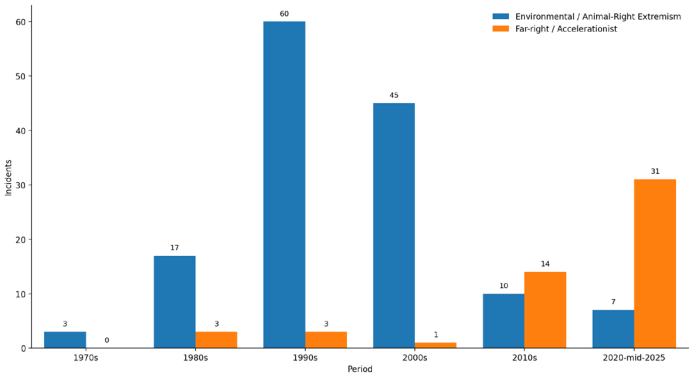

Figure 1: The temporal distribution of incidents in the core dataset, highlighting two distinct waves: a late-1990s peak associated with environmental and animal-rights extremism and a post-2015 rise in infrastructure plotting linked to far-right extremist and accelerationist actors. (N=194)

Analysis of this type of data has inherent limitations. Some of these limitations include undercounting and selection bias inherent in open-source and court-record based compilation, as well as ambiguity in attributing ideology and target classification in mixed-motive or poorly documented cases. Foiled-plot coverage is also time-skewed because disrupted plots are far more likely to be documented publicly in recent decades than in the 1970s and 1980s. To avoid using 'accelerationism' as a catch-all, cases were coded as accelerationist only when primary-source case materials evidenced accelerationist framing, such as explicit collapse-catalysis language, references to accelerationist texts or communities,

a According to the Cybersecurity and Infrastructure Security Agency (CISA), "there are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." The sectors are Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Services and Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems. "Critical Infrastructure Sectors," Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Homeland Security, updated 2024.

or communications describing infrastructure disruption as a mechanism to accelerate societal breakdown.

Incident Tally and Trends

Between 1970 and mid-2025, the core dataset used in this article identifies 194 infrastructure-related incidents, including both completed attacks and foiled plots, motivated by domestic extremist ideologies.[b] The overwhelming majority fall into two main ideological categories. The first is environmental and animal-rights extremism, which accounts for 142 of the 194 cases and peaks in the late 1990s and early 2000s. This infrastructure-focused subset overlaps with the much larger ELF/ALF arson-and-bombing campaign documented elsewhere, including 239 significant arsons or bombings between 1995 and 2010, though not all of those broader incidents meet this article's infrastructure-targeting criteria. The second is far-right, anti-government, and accelerationist extremism, which accounts for 52 of the 194 cases and rises markedly after 2015.[9] While a considerable portion of these incidents targeted infrastructure, not all of them did. These incidents peaked in the late 1990s, specifically between 1998 and 2001, before declining sharply after 2005. Importantly, few of these attacks were intended to harm human life, and perpetrators frequently emphasized property destruction over casualties. Statements issued by ELF and ALF cells routinely framed arson and sabotage as a means of inflicting economic costs, deterring specific practices, and drawing attention to environmental or animal-rights grievances rather than as an effort to cause physical harm.[10] Despite that restraint, the property damage was substantial: In one DHS assessment that reviewed the 1995-2010 period, 42 percent of attacks were classified as causing "substantial or very substantial" loss.[11]

The second category involves far-right, anti-government, and accelerationist extremism, which began to rise markedly after 2015. A growing number of plots against critical and infrastructure-adjacent targets have been linked to far-right domestic violent extremists, including white supremacists, neo-Nazi accelerationist cells, and anti-government militias.[12] Between 2016 and 2022, the Program on Extremism at George Washington University identified 35 federal cases involving violent extremist plots against critical infrastructure, including 16 associated with white supremacist actors; 13 of those white supremacist plotters specifically targeted the energy sector.[13] The frequency of such plots has further spiked in recent years, rising from one or two cases annually between 2016 and 2018 to double digits after 2020.[14] Where case materials explicitly show accelerationist intent, grid attacks are framed as a symbol and strategic target that, at least in the perpetrator's view, could facilitate broader systemic collapse.[15]

Target selection and methods vary between these ideological streams and eras. Eco-extremists in the 1970s through early 2000s tended to focus on symbols of environmental destruction or animal exploitation. According to DHS analysis of bombing and arson incidents attributed to the ELF and ALF milieu, 55 percent were claimed under the ELF name and 45 percent under the ALF name. Nearly two-thirds of these incidents occurred in the U.S. West, particularly in the Pacific Northwest (PNW) and California.[16] Their targets included timber company offices, meatpacking plants, university laboratories, SUV dealerships, and residential developments—occasionally extending to energy infrastructure when connected to fossil fuel or nuclear projects. Their tactics primarily involved arson and bombing, with 62 percent bombings and 38 percent arsons in a 1995 to 2010 DHS dataset, often using delayed timers and improvised incendiary devices. In infrastructure-adjacent cases, methods also included equipment sabotage such as damaging fuel lines or disabling machinery tied to targeted facilities.[17] In that same DHS 1995-2010 dataset, attacks were generally planned for times when facilities were unoccupied.

In this study's 1970 to mid-2025 dataset, far-right extremist and accelerationist actors who targeted infrastructure focused most often on the electric grid, particularly substations, transformers, and transmission lines. DOJ cases and DHS assessments show that white-supremacist conspirators view power stations as high-value targets capable of producing cascading chaos.[18] In one 2020 case, a neo-Nazi cell in Ohio plotted to shoot transformers to induce blackouts.[19] Other targets have included telecommunications towers, rail lines, and water systems.[20] The methods associated with these actors are often cruder but carry greater risk of lethal harm, including rifle fire directed at transformers, pipe bombs, and the use of commercially available explosive compounds such as Tannerite.[c] Unlike earlier eco-sabotage campaigns, several recent far-right extremist and accelerationist plots frame infrastructure disruption as a means to generate broader instability. In the 2023 Baltimore substation conspiracy, for example, one plotter described the objective as to "completely destroy this whole city," reflecting an accelerationist logic that treats infrastructure disruption as a pathway to cascading societal effects.[21] Compared with earlier eco-sabotage campaigns, these actors appear less focused on minimizing casualty risk, and some cases involve multi-site attack concepts intended to magnify disruption and complicate emergency response.[22]

Viewed at a high level, the dataset reveals clear geographic and temporal clustering patterns, alongside shared dynamics in how small-scale sabotage can generate outsized disruption. Geographically, eco-extremist incidents were concentrated in the U.S. West—Oregon, Washington, California, and Colorado—while far-right extremist infrastructure plots and attacks have been dispersed more widely across the Southeast, Midwest, and Pacific Northwest. Temporal spikes in this type of activity align with broader periods of unrest: Eco-terrorism peaked in the late 1990s before subsiding, whereas far-right extremist plots surged after 2020 amid pandemic-related volatility, civil protests, and deepening polarization. While overall fatalities remain rare in infrastructure attacks, modern grid disruptions carry far greater potential to endanger lives through secondary effects such as power outages. Prosecution trends reflect this divergence: Eco-saboteurs of the early 2000s often received sentences under 10 years, whereas recent far-right extremist offenders faced terrorism-enhanced

b The core dataset analyzed in this article includes N=194 coded cases involving attacks and plots against U.S. critical infrastructure and infrastructure-adjacent industrial and commercial targets. A broader reference universe of cases was reviewed during compilation, but adjacent, ambiguous, or non-qualifying incidents were excluded from the final analytic dataset.

c Tannerite is a commercially sold "binary exploding target" product. It typically comes as two separate components, commonly an oxidizer such as ammonium nitrate and a fuel such as aluminum powder, that are mixed by the user and can detonate when initiated, often by impact from a high-velocity rifle round.

penalties of up to 20 years.[23]

Historical Trajectory by Decade: From Eco-Sabotage to Accelerationism

1970s: Beginnings of Eco-Radicalism

The dataset records just three infrastructure-related extremist incidents in the 1970s, all linked to early eco-radicalism. No far-right extremism or accelerationist plot that focused on infrastructure as a target appears in the dataset during this period.

The 1970s were the formative decade for modern U.S. environmental politics and, at the militant fringe, for the ideas that later underpinned eco-sabotage. The first Earth Day in 1970 helped catalyze mass environmental awareness, and a rapid expansion of federal environmental regulation followed, including the National Environmental Policy Act and the creation of the Environmental Protection Agency.[24] For most activists, these developments reinforced lawful advocacy. For a smaller militant subset, they reinforced the belief that conventional politics was too slow to prevent irreversible harm, creating a permissive logic for property destruction framed as defensive direct action.

The term "ecotage" gained currency in this period, popularized by the 1972 publication Ecotage! and reinforced culturally by Edward Abbey's novel *The Monkey Wrench Gang* (1975), which depicted sabotage of development as a form of resistance.[25] This outlook began to translate into real-world activity by the late 1970s. One early U.S. example frequently cited in open sources is a 1977 laboratory break-in at the University of California, Riverside attributed to a group described as the "Undersea Railroad," which released animals and destroyed equipment.[26] This attack established patterns that later defined eco-extremist campaigns: clandestine entry, nighttime operations, and an emphasis on property destruction rather than casualties.

On the far-right extremism side, violence in the 1970s was generally not oriented toward sustained infrastructure sabotage. More often, it focused on people, demonstrations, and symbolic adversaries through intimidation and lethal violence tied to racial terror and ideological conflict. The 1979 Greensboro massacre, in which Klansmen and neo-Nazis killed five Communist Workers Party demonstrators at an anti-Klan protest, illustrates that broader targeting pattern. More generally, U.S. terrorism in the 1970s was dominated by left-wing and Puerto Rican nationalist violence rather than the infrastructure-centered far-right extremism plotting that became more visible decades later.[27]

1980s – Radicalization and Early Infrastructure Attacks

From 1980 to 1989, the dataset captures 20 incidents, with 17 linked to environmental or animal-rights extremism and three involving early infrastructure plotting tied to individuals or groups motivated by far-right extremist ideologies.

During the 1980s, militant environmentalism shifted from fringe protest toward a more coherent movement that promoted direct action and, for a minority, sabotage as a legitimate tool of environmental defense. Earth First!, founded in 1980, helped drive this turn by rejecting compromise-oriented environmentalism and elevating confrontation as a method rather than an exception.[28] Over the decade, tactics became more adversarial, including the adoption of tree-spiking by the mid-1980s to deter logging, a practice that also increased risk to workers and equipment. In 1987, Earth First! activists sabotaged a transmission tower supplying power to a uranium mine in Arizona, further illustrating how movement rhetoric could translate into attacks on infrastructure tied to extractive industries.[29]

Animal-rights militancy also escalated. The ALF expanded laboratory raids and arsons, including a 1982 firebombing at a University of California, Davis facility, and in 1987 the FBI publicly warned of the "increasing violence of animal rights extremists."[30] On the far-right extremism side, concepts that later enabled infrastructure-focused violence also diffused, including Louis Beam's "leaderless resistance," while groups linked to Christian Identity ideology, such as The Covenant, The Sword, and the Arm of the Lord, plotted attacks on pipelines and water supplies.[31] These developments did not yet produce sustained infrastructure sabotage at scale, but they helped set conditions for the more systematic targeting that emerged later.

1990s – The Eco-Terrorism Wave ("Green Scare")

The 1990s saw a sharp increase in eco-extremist activity, with the dataset recording 60 incidents linked to ELF/ALF campaigns and three early far-right extremist plots, totaling 63 infrastructure-related acts. As shown in Figure 2, eco-extremist actors accounted for the overwhelming majority of infrastructure-related incidents during this period.

The late 1990s marked the peak of eco-terrorism activity in the United States. The ELF emerged and expanded from the United Kingdom and rapidly escalated sabotage. In one key incident, on October 19, 1998, ELF saboteurs ignited multiple incendiary devices at Vail Mountain (Colorado), burning down the Two Elk lodge and several ski lifts, causing approximately $12 million in damage.[32] The group was careful to avoid human casualties, crafting their attacks at night in empty facilities. In early 2002, FBI Domestic Terrorism Chief James Jarboe testified that ALF/ELF had committed over 600 criminal acts since 1996 and that "special interest extremists" were the most active domestic threat.[33]

The Vail arson also illustrates a broader tactical and organizational pattern that defined the late 1990s wave. ELF and ALF activity relied on autonomous cells operating under a shared banner rather than a formal hierarchy, which complicated attribution and made the movements resilient to leadership decapitation strategies. Attacks often followed a recognizable script:

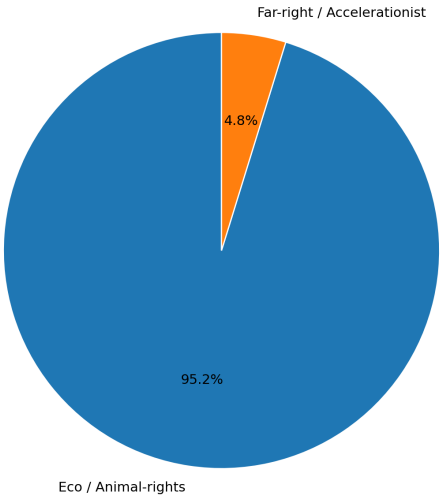

Figure 2: Distribution of extremist attacks and plots against U.S. critical infrastructure and infrastructure-adjacent industrial and commercial targets by ideological category, 1990–1999 (n=63)

clandestine surveillance of a target linked to a specific grievance, deployment of improvised incendiary devices with delayed timers, and rapid dissemination of anonymous communiqués that framed the action as defensive and morally necessary. The cumulative effect was less about seizing territory or confronting the state directly and more about coercion through economic cost, reputational damage, and deterrence. This pattern also helps explain why the same period produced comparatively few casualties but substantial property loss, and why federal counterterrorism efforts increasingly treated "special interest" extremism as a priority threat category even before the post-9/11 reorientation toward Islamist terrorism.[34]

2000s – Lull and Transition

From 2000 to 2009, the dataset documents 45 eco-extremist incidents—including many tied to Operation Backfire investigations—and one case attributed to far-right extremist actors, for a total of 46 incidents of infrastructure-focused targeting by these two threat streams.

The early 2000s were still an active period for eco-extremist sabotage, even as the wave began to crest. High-profile arsons continued into the first half of the decade, and federal investigations increasingly treated ALF/ELF activity through a post-9/11 domestic terrorism lens, leveraging conspiracy, destructive-device, and terrorism-related charging and sentencing tools that raised the stakes for participants and supporters.[35] Operation Backfire (2004-2008) dismantled the core Pacific Northwest eco-extremist cell network known among investigators as "The Family," which carried out numerous ELF and ALF arsons in the late 1990s and early 2000s.[36] A few outlier acts occurred (for example, the 2008 Seattle-area "Street of Dreams" arson), but overall activity dropped sharply.[37]

Legal tools also expanded when Congress passed the Animal Enterprise Terrorism Act in 2006, broadening 18 U.S.C. § 43 and increasing penalties tied to economic damage and threats.[38] While the deterrent effect is difficult to prove conclusively, multiple analyses of Operation Backfire and post-crackdown trends find a substantial decline in activity consistent with a disruption-and-deterrence dynamic.[39] Infrastructure security also improved in response to non-adversarial system shocks, including the 2003 Northeast blackout. On the far-right extremism side, post-2008 economic dislocation and the Obama presidency contributed to radicalization; infrastructure attacks were still rare, but episodic incidents and nascent plotting began to appear.[40] This decade was the calm before the new storm.

2010s – Renewed Extremism and Convergence of Tactics

Between 2010 and 2019, 24 infrastructure-focused incidents are recorded in the dataset: 10 attributed to eco-anarchist actors, and 14 to far-right extremists or accelerationists.

The 2010s saw two related developments: a resurgence and adaptation of eco-anarchist sabotage tied to energy and pipeline opposition, and the emergence of accelerationism, often linked with far-right extremist ideas, as a distinct organizing logic.[41] The 2013 sniper attack on the PG&E Metcalf substation in California (still unsolved) became a template for grid attackers.[42] Members and supporters of accelerationist neo-Nazi networks such as the Atomwaffen Division (founded 2015) circulated online guides and discussed tactics for attacking the power grid, sharing instructions on identifying and disabling transformers and other substation

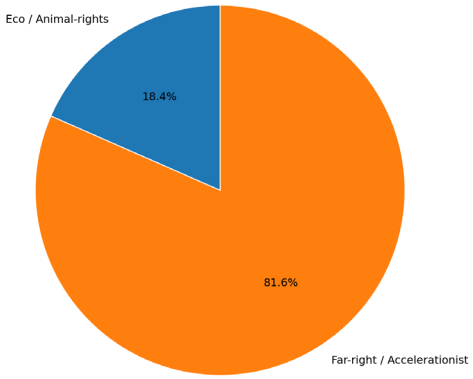

Figure 3: Distribution of extremist attacks and plots against U.S. critical infrastructure and infrastructure-adjacent industrial and commercial targets by ideological category, 2020–2025 (n=38)

equipment that could be damaged by rifle fire or explosives.[43] Eco-extremist movements had already normalized leaderless sabotage by the 1990s; during the 2010s, far-right extremist groups increasingly borrowed both this decentralized model and specific sabotage techniques, including arson and infrastructure-focused attacks. By contrast with the much larger late-1990s eco-sabotage wave, eco-extremist activity in the United States during the 2010s appears limited to a small number of isolated sabotage incidents, likely fewer than a dozen, often tied to energy and pipeline opposition. By the 2010s, however, infrastructure disruption was no longer confined to that milieu and increasingly appeared across ideological contexts.[44]

2020-Mid-2025 – Accelerationist Grid Targeting and Renewed Eco-Anarchist Sabotage

The period from 2020 through mid-2025 accounts for 38 incidents, with 31 attributed to far-right extremist or accelerationist actors and seven involving renewed eco-anarchist sabotage. Figure 3 highlights the distribution of recent incidents across ideological categories, underscoring the rise of far-right extremist and accelerationist-linked infrastructure plotting in the current period.

The COVID-19 pandemic, civil unrest, election polarization, and conspiracy ecosystems created permissive conditions for infrastructure targeting across ideologies. On the far-right extremism side, several cases reflected an accelerationist logic that treats grid disruption as a high-leverage way to strain governance and amplify social breakdown. In December 2022, the Moore County, North Carolina, substation shootings caused a serious outage affecting approximately 45,000 customers.[45][d] In the Pacific Northwest, a late 2022 series of attacks near Tacoma, Washington, damaged multiple substations and produced significant outages, underscoring how small teams can generate outsized disruption.[46] In early 2023, authorities disrupted the Baltimore-area grid plot, and in August 2025, plotter Brandon Russell was sentenced to 20 years in federal prison for conspiring to destroy electrical facilities serving the region.[47]

In parallel, what this article calls modern eco-anarchy is not a new ideology so much as a renewed, decentralized current of anti-

d While it is widely speculated that the perpetrators of the Moore County substation attack were right-wing extremists, the shooters have not been apprehended as of March 19, 2026.

industrial direct action that targets energy and extractive supply chains, including fossil-fuel logistics, rather than pursuing mass-casualty violence. A concrete example is the 2020 Washington State rail "shunts" case, where federal charges alleged the use of devices placed on BNSF Railway tracks to interfere with signaling and trigger emergency braking, including for trains carrying hazardous materials.[48]

Comparative Analysis: Eco-Extremism vs. Accelerationist Extremism

This section compares two distinct threat milieus that sometimes produce superficially similar operational patterns but differ in their theory of change, targeting logic, and risk profile. The table below summarizes common tendencies, not hard rules, and there is meaningful variation within each category. Importantly, 'accelerationism' is used here as a strategic logic aimed at hastening systemic breakdown, not as a synonym for the broader far-right extremist milieu. The comparison focuses on far-right extremist actors whose case materials or propaganda explicitly reflect that accelerationist logic.

Table 1: Comparative Dimensions of Eco-Extremist and Far-Right Accelerationist Infrastructure Targeting

Dimension	Left-Wing Eco-Extremism (ELF/ALF)	Far-Right Extremist/Accelerationist Actors (subset of far-right extremism)
Core Motive/ Theory of Change	Issue-driven coercion tied to environmental or animal-rights grievances; impose economic costs, deter specific practices, force attention	System-disruption logic; accelerate breakdown, erode legitimacy, provoke cascading failure and social conflict (including anti-state and race-war narratives in many cases)
Targeting Logic	Predominantly commercial, industrial, and research targets linked to grievance (timber, labs, construction, dealer-ships, processing facilities); critical-infrastructure or infrastructure-adjacent targets when directly tied to extractive/energy disputes	Critical nodes prioritized for cascading effects, especially electric substations, transformers, and transmission lines; secondary enabling nodes may include telecoms, rail choke-points, and water-related facilities
Typical Tactics	Arson and improvised incendiary devices; sabotage of facilities/equipment; delayed ignition/time-setting common; firearms generally avoided	Firearms against electrical equipment; IEDs/explosives and sabotage; multi-site coordination concepts; hybrid physical-cyber ideas appear in some discourse and plotting
Casualty Risk Posture	Often calibrated to reduce probability of casualties (night operations, unoccupied targets), though risk remains inherent	Higher tolerance for risk of lethal harm; means and concepts often increase likelihood of casualties to responders, bystanders, or workers even when deaths do not occur
Organization	Leaderless resistance/autonomous cells operating under a shared banner; weak central command by design	Decentralized but digitally networked; loose online ecosystems and small cells; inspiration and guidance often diffuse through propaganda and tactical content
Communications	Anonymous communiqués, underground media, moral-justification framing; early internet use	Encrypted chats, forums, manifestos and tactical guides; memes and propaganda optimized for diffusion and replication
Operational Cadence and Geography (Typical)	Concentrated historically in the West (PNW/California/Colorado) with episodic spikes (late 1990s–early 2000s)	More geographically dispersed; noticeable post-2015 rise with spikes after 2020; repeated focus on grid targets in multiple regions

Three differences matter operationally. First, target type: Eco-extremists often select grievance-linked commercial or industrial nodes where disruption is symbolic and economically punitive, whereas accelerationist actors prioritize high-leverage critical nodes where they view potential for failure to cascade across communities. Second, risk posture: Eco-sabotage has historically tried to reduce the probability of casualties through timing and target selection, while accelerationist plotting tolerates higher casualty risk and frequently relies on firearms or high-energy explosives. Third, theory of change: Eco-sabotage is typically coercive and issue-

bounded, whereas accelerationism is system-disruptive and aims to amplify instability, polarize communities, and erode state capacity.

Areas of convergence are noteworthy not because eco-extremist movements and actors employing accelerationist logic share the same ideological goals, but because both have at times relied on similar operational methods of sabotage against infrastructure. Eco-extremist sabotage and infrastructure-focused accelerationist plotting are distinct phenomena, not parallel movements with shared goals. Eco-extremism is usually issue-specific and coercive, using sabotage to impose costs and deter practices viewed as environmentally destructive. Accelerationist actors, by contrast, treat attacks on infrastructure as a means of producing broader systemic disruption or collapse. The comparison is still useful at the operational level: Both have at times relied on decentralized organization, clandestine cells, and sabotage against high-visibility targets. But the differences are more important than the similarities. Eco-extremist campaigns historically focused more often on grievance-linked commercial or infrastructure-adjacent assets, whereas accelerationist actors more often target truly critical systems, especially the electric grid, for their cascading effects.

Law-Enforcement and Policy Response Trajectory (2000-2025)

This section summarizes how federal and state responses have evolved as the center of gravity in domestic infrastructure sabotage shifted. It traces the transition from early 2000s "special interest" cases associated with environmental and animal-rights extremism to the late-2010s and 2020s focus on domestic violent extremists (including racially or ethnically motivated actors) and critical infrastructure risk. The throughline is not only changing adversaries, but changing legal tools, intelligence posture, and the degree to which infrastructure protection became integrated into counterterrorism practice.

Operation Backfire (2004-2008)

The FBI's Operation Backfire dismantled the core Pacific Northwest network known as "The Family," which had carried out high-profile arsons and related sabotage under the ELF and ALF banners. The investigation solved more than 40 eco-terrorism crimes, leading to the indictment of 11 members and guilty pleas from over 15 individuals by late 2007, with sentences of up to 13 years in federal prison.[49] Courts applied terrorism enhancements even though no deaths occurred, reflecting an expansive understanding of terrorism that includes ideologically motivated property destruction; critics argued this blurred distinctions between sabotage campaigns and mass-casualty terrorism, and the debate persists.[50]

Legislation Adaptation

In 2006, Congress passed the Animal Enterprise Terrorism Act (AETA) to enhance penalties for sabotage tied to animal-related industries; the statute implicitly accepted that ideological property destruction could be terrorism.[51] Infrastructure protection efforts also became more formalized and enforceable. After the Energy Policy Act of 2005, the Federal Energy Regulatory Commission (FERC) gained authority to oversee mandatory reliability standards for the bulk power system, and the North American Electric Reliability Corporation (NERC)'s Critical Infrastructure Protection (CIP) standards became the backbone of regulated grid security.[52] Later, after heightened concern about physical attacks on substations, FERC directed development of a dedicated physical-security reliability standard (CIP-014), requiring certain transmission owners to identify critical facilities and implement physical security plans.[53]

Intelligence Adaptation, Prosecution Strategies, and Reporting

By the late 2010s and early 2020s, the U.S. intelligence community and DHS/FBI increasingly framed domestic violent extremists as a sustained terrorism threat with credible pathways to critical infrastructure targeting, including the energy sector.[54] Senior DHS intelligence leadership explicitly distinguished between routine vandalism and ideologically driven grid attacks, warning that some incidents are conducted by DVEs seeking to "engineer a societal collapse."[55] Prosecution strategy also shifted toward infrastructure-specific charging. Section 1366 of the U.S. Code (destruction of an energy facility) has become a central tool in major grid plots, including the Baltimore-area conspiracy that resulted in a 20-year federal sentence.[56] In parallel, threat reporting to the private sector became more institutionalized through sector coordinating mechanisms, Information Sharing and Analysis Center (ISAC) channels, and fusion-center dissemination, reducing reliance on ad hoc warning pathways.[57]

Gaps and Considerations

Key challenges persist: The United States lacks a federal domestic terrorism statute for ideologically motivated violence not tied to a foreign group; many small utilities lack resources to harden infrastructure; public-private intelligence-sharing remains inconsistent; and many state-level law-enforcement agencies remain oriented toward vandalism rather than ideologically motivated targeted sabotage.[58] Despite episodic attention, infrastructure-focused domestic extremism is still often handled in ideological stovepipes, and cross-ideological threat modeling, prioritization, and sustained resourcing remain uneven across agencies and jurisdictions.[59]

Conclusion

The phenomenon of 'two extremes, one grid' reveals that critical infrastructure and adjacent industrial/commercial targets have become a shared battlefield for extremist movements motivated by differing ideologies. While their worldviews could not differ more, both share interest in the same general target set—not by accident, but because infrastructure holds power in its symbolism—something all of society relies on—which makes it a highly attractive target for disruption and spectacle, and, at least in the eyes of some, to catalyze. Importantly, this partial overlap in target sets creates a strategic opportunity: Measures that harden core grid assets against one category of extremist yield spillover protection against others, even though eco-extremists and accelerationist actors have historically prioritized different types of infrastructure and pursued different strategic ends.

Although this article presents eco-extremism and accelerationist violence as distinct analytical categories, real-world actors do not always fall neatly into one camp. Some recent cases reflect ideological crossover or tactical borrowing, such as individuals adopting both anti-industrial and anti-state framing. Online ecosystems have accelerated this blending by circulating sabotage manuals, manifestos, and visual propaganda across ideological lines. Future threat modeling and policy planning should account for this fluidity, particularly as lone actors and decentralized cells increasingly draw from multiple extremist milieus.

This review of 50 years of domestic infrastructure terrorism shows that attacks on U.S. infrastructure have emerged in distinct ideological waves rather than along a single continuous trajectory. Environmental and animal-rights extremism dominated the late 1990s and early 2000s, while far-right extremism infrastructure plotting, including a subset of explicitly accelerationist cases, rose after 2015. These waves differed in target selection, methods, and theory of change: Eco-extremist campaigns more often focused on grievance-linked commercial and industrial targets and generally emphasized coercive economic disruption, whereas contemporary accelerationist actors have more often prioritized critical systems, especially the electric grid, for their potential to produce cascading effects. The broader implication is that infrastructure sabotage should be understood as a recurring tactic that can migrate across ideological milieus even when motives and strategic objectives differ. Effective policy therefore requires both precision and breadth: precision in distinguishing among perpetrators and pathways to violence, and breadth in building protective and resilience measures that remain useful across changing threat environments. CTC

Citations

1 "White Supremacist Leader Found Guilty of Conspiring to Destroy Regional Power Grid," U.S. Department of Justice, February 3, 2025.
2 "Arson at the Vail Ski Resort, 1998," Intermountain Histories, Utah State University, 2024.
3 Steven M. Chermak, Joshua D. Freilich, Celinet Duran, and William S. Parkin, *An Overview of Bombing and Arson Attacks by Environmental and Animal Rights Extremists in the United States, 1995–2010* (College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), U.S. Department of Homeland Security Science & Technology Directorate, May 2013.
4 "Testimony of James F. Jarboe, Domestic Terrorism Section Chief, Counterterrorism Division, FBI," before the House Resources Subcommittee on Forests and Forest Health, February 12, 2002.
5 Seamus Hughes and Alexander Meleagrou-Hitchens, "'It's Going to be a Show': White Supremacist Plots Targeting Critical Infrastructure," Program on Extremism, George Washington University, February 2023.
6 *Homeland Threat Assessment 2024* (Washington, D.C.: DHS, September 2023), p. 23.
7 Ibid.; *Setting Fires for Effect: A Journal of the Earth Liberation Front* 1 (2001), Earth Liberation Front Press Office, archived by the FBI.
8 "Domestic Extremism Tracker," Program on Extremism, George Washington University, accessed January 15, 2026.
9 Chermak, Freilich, Duran, and Parkin.
10 James F. Jarboe, "The Threat of Eco-Terrorism," Statement before the House Resources Committee, Subcommittee on Forests and Forest Health, U.S. House of Representatives, Washington, D.C., February 12, 2002.
11 Chermak, Freilich, Duran, and Parkin, p. 5.
12 *Homeland Threat Assessment 2024*, pp. 21-23.
13 Ilana Krill and Bennett Clifford, *Mayhem, Murder, and Misdirection: Violent Extremist Attack Plots Against Critical Infrastructure in the United States, 2016-2022* (Washington, D.C.: Program on Extremism, George Washington University, September 2022).
14 Ibid.
15 Ibid.
16 Ibid.
17 Chermak, Freilich, Duran, and Parkin.
18 *Homeland Threat Assessment 2024*, pp. 22-23; "White Supremacist Leader Found Guilty of Conspiring to Destroy Regional Power Grid."
19 "Two Men Sentenced for Conspiring to Provide Material Support to Plot to Attack Power Grids in the United States," U.S. Department of Justice, April 21, 2023.
20 U.S. Cybersecurity & Infrastructure Security Agency and related industry reporting on telecom attacks linked to conspiracy movements and violence against cellular towers, including DHS warning about 5G-related attacks on telecommunications infrastructure, cited in research on extremist targeting; "Huge Potential for Terror on Rail Lines Touted in Accelerationist Attack Tutorial," Homeland Security Today, July 28, 2022, detailing explicit accelerationist guidance for attacking rail infrastructure as part of a broader sabotage strategy.
21 "Maryland Woman and Florida Man Charged with Conspiring to Attack Electrical Substations in the Baltimore Region," U.S. Department of Justice, February 6, 2023.
22 *Homeland Threat Assessment 2024*, pp. 22-23.
23 "White Supremacist Leader Found Guilty of Conspiring to Destroy Regional Power Grid."
24 "The Birth of EPA," accessed February 2026; National Environmental Policy Act of 1969, Pub. L. No. 91-190, 83 Stat. 852 (1970); Adam Rome, *The Genius of Earth Day: How a 1970 Teach-In Unexpectedly Made the First Green Generation* (New York: Hill and Wang, 2013).
25 Bron Taylor, "Religion, Violence and Radical Environmentalism: From Earth First! to the Unabomber to the Earth Liberation Front," *Terrorism and Political Violence* 10:4 (1998): pp. 1-42.
26 Federal Bureau of Investigation, *Terrorism in the United States: 1999*, FBI Counterterrorism Division, discussion of early animal-rights direct-action precedents, including the 1977 University of Hawaii dolphin release.
27 *Patterns of Terrorism in the United States, 1970–2013* (College Park, MD: START, University of Maryland, 2014), prepared for the U.S. Department of Homeland Security, Office of University Programs; William S. Powell ed., "Death to the Klan March," NCpedia, University of North Carolina Press, accessed March 11, 2026.
28 Dave Foreman, "Confessions of an Eco-Warrior," Earth First! Journal, early founding statements, 1981–1983, describing the movement's opposition to compromise environmentalism and embrace of confrontation.
29 *Terrorism in the United States: 1987* (Washington, D.C.: FBI, Counterterrorism Section, 1988), discussion of Earth First–associated sabotage incidents involving energy and mining infrastructure in the Southwest. See also Taylor, pp. 9-11, referencing the 1987 Arizona transmission-tower sabotage tied to uranium mining.
30 *Terrorism in the United States: 1987*, discussion of animal-rights extremism and laboratory arsons. See also Federal Bureau of Investigation testimony, "The Threat of Animal Rights Extremism," before Congress, 1987, referencing the UC Davis firebombing and warning of escalating violence.
31 Louis Beam, "Leaderless Resistance," *The Seditionist* 12 (1992), foundational essay outlining decentralized violence concepts that later diffused widely; *Terrorism in the United States: 1985* (Washington, DC: FBI, 1986), discussion of The Covenant, The Sword, and the Arm of the Lord and plots involving attacks on pipelines and water supplies; J. M. Berger, *Extremism* (Cambridge, MA: MIT Press, 2018), chap. 4, situating Christian Identity groups and early infrastructure-adjacent plotting within the broader far-right extremism ecosystem.
32 "Five Members of Earth Liberation Front Indicted for 1998 Vail Arson," U.S. Department of Justice, February 7, 2006.
33 James F. Jarboe, "The Threat of Eco-Terrorism," Statement before the House Resources Committee, Subcommittee on Forests and Forest Health, U.S. House of Representatives, Washington, D.C., February 12, 2002.
34 *Terrorism in the United States: 1998* and *1999*, Federal Bureau of Investigation, sections on "Special Interest Extremism," which explicitly rank eco-terrorism and animal-rights extremism as leading domestic threats prior to 2001.
35 "Eleven Defendants Indicted on Domestic Terrorism Charges," U.S. Department of Justice, January 20, 2006.
36 "Operation Backfire," speech/remarks, Federal Bureau of Investigation, November 19, 2008.
37 "Seattle Eco-Terrorism Investigation," Federal Bureau of Investigation, March 4, 2008.
38 Animal Enterprise Terrorism Act, Pub. L. No. 109–374, 120 Stat. 2652 (2006).
39 *The Case of "Operation Backfire"* (College Park, MD: START, 2012), on disruption effects and post-operation decline. See also evidence of countermeasure effectiveness in subsequent quantitative evaluations of post-intervention eco-terrorism trends.

40 *U.S.–Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* (Washington, D.C. and Ottawa: U.S. Department of Energy and Natural Resources Canada, April 2004); Arie Perliger, *American Zealots: Inside Right-Wing Domestic Terrorism* (New York: Columbia University Press, 2020), pp. 134-139.
41 "Two Des Moines Women Plead Guilty to Conspiracy to Damage Energy Facilities," U.S. Department of Justice, July 9, 2021; *Homeland Threat Assessment 2024*, pp. 22–24.
42 Jon Wellinghoff, "Physical Security of the U.S. Power Grid: Lessons from the Metcalf Attack," Federal Energy Regulatory Commission Testimony, April 10, 2014. See also Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," *Wall Street Journal*, February 5, 2014.
43 Krill and Clifford, pp. 4-5.
44 The Case of "Operation Backfire;" "Operation Backfire," Federal Bureau of Investigation; "Valve Turner Who Shut Down Minnesota Pipelines Sentenced," U.S. Department of Justice, October 30, 2018; Global Terrorism Database.
45 "Shooting of Electrical Substations," FBI bulletin, December 3, 2022.
46 Robert Walton, "Puget Sound Energy, Tacoma Power Substations Damaged in Christmas Day Attacks," Utility Dive, December 26, 2022; "Christmas Brings New Round of Attacks on Northwest Power Grid," KUOW, December 25, 2022.
47 "Florida Man Sentenced to 20 Years for Conspiring to Destroy Baltimore Region Power Grid," U.S. Department of Justice, U.S. Attorney's Office for the District of Maryland, August 7, 2025; "Neo-Nazi Group Leader Sentenced to 20 Years in Prison for Planned Maryland Power Grid Attack," Associated Press, August 7, 2025.
48 "Pair Charged with Interfering with Safety on Railroad Tracks," U.S. Department of Justice, U.S. Attorney's Office for the Western District of Washington, November 30, 2020.
49 "Operation Backfire: Thirteen Defendants Indicted for Series of Eco-Terrorist Attacks," U.S. Department of Justice, January 20, 2006; "Sentencings in Operation Backfire Cases," U.S. Department of Justice, November 20, 2007.
50 David Thomas Sumner and Lisa M. Weidman, "Eco-Terrorism or Eco-tage: An Argument for the Proper Frame," *Interdisciplinary Studies in Literature and Environment* 20:4 (2013): pp. 857-876.
51 Animal Enterprise Terrorism Act; "Overview of the Animal Enterprise Terrorism Act," Office of Legal Policy Briefing Paper, U.S. Department of Justice, 2007.
52 "Cyber and Grid Security," Federal Energy Regulatory Commission, explaining FERC's authority under the Energy Policy Act of 2005 to approve mandatory reliability standards, including cybersecurity standards for the bulk power system; North American Electric Reliability Corporation, "History of NERC" (timeline), noting FERC approval of the first version of NERC's CIP Reliability Standards in January 2008.
53 Federal Energy Regulatory Commission, "Physical Security Reliability Standard," *Federal Register* 79:141 (2014), describing proposed Reliability Standard CIP-014-1 submitted in response to the Commission's March 7, 2014, order; "High-Voltage Transformer Substations," Congressional Research Service, 2015, summarizing FERC approval of mandatory physical security standard CIP-014-1 and its requirements for certain transmission owners.
54 *Domestic Violent Extremism Poses Heightened Threat in 2021*, Office of the Director of National Intelligence, unclassified summary, March 1, 2021; *Strategic Intelligence Assessment and Data on Domestic Terrorism*, Federal Bureau of Investigation and U.S. Department of Homeland Security, May 2021.
55 Kenneth L. Wainstein, Under Secretary for Intelligence and Analysis, U.S. Department of Homeland Security, interview remarks on domestic violent extremists and power-grid attacks, February 2023 (as reported by national media).
56 "Florida Man Sentenced to 20 Years for Conspiring to Destroy Baltimore Region Power Grid."
57 "The Rising Threat of Domestic Terrorism in the U.S. and Federal Efforts to Combat It," U.S. Government Accountability Office, March 2, 2023, discussion of federal information-sharing and coordination efforts; *Strategic Intelligence Assessment and Data on Domestic Terrorism*, U.S. Department of Homeland Security, October 2022, sections on information-sharing and engagement with private-sector partners.
58 *Domestic Terrorism: An Overview* (Washington, D.C.: Congressional Research Service, updated multiple years), discussing the absence of a standalone domestic terrorism statute and reliance on workaround charges; *Critical Infrastructure Protection: Additional Federal Actions Could Help Address Cybersecurity and Physical Security Challenges Faced by Small Utilities* (Washington, D.C.: GAO, 2023); *Strategic Intelligence Assessment and Data on Domestic Terrorism*, noting persistent challenges in information sharing with private-sector owners and operators; Terrorism in the United States, Federal Bureau of Investigation (annual reports, late 1990s–2000s) and subsequent DHS assessments, documenting recurring treatment of infrastructure attacks as criminal mischief or vandalism absent clear ideological indicators.
59 *Countering Domestic Terrorism: Additional Actions Needed to Strengthen Federal Efforts* (Washington, D.C.: Government Accountability Office, 2023); *DHS Needs a Comprehensive Strategy to Counter Domestic Terrorism* (Washington, D.C.: DHS OIG, 2022).