Cross-Sector ISAC Physical Security Report: Recent Extremist Publications and Their Impact on the Critical Infrastructure Threat Landscape

April 2024

This report involved cross-sector analysts from the following ISACs:

- Electricity Information Sharing and Analysis Center
- Health Information Sharing and Analysis Center
- Water Information Sharing and Analysis Center
- Financial Services Information Sharing and Analysis Center
- Downstream Natural Gas Information Sharing and Analysis Center
- Public Transportation, Over the Road Bus, and Surface Transportation Information Sharing and Analysis Centers

Contents

Introduction

During Q1 2024, the Electricity Information Sharing and Analysis Center (E-ISAC) became aware of two extremist publications that focused on the electric grid and other critical infrastructure. The documents, titled *Redstone Killers* and *The Known Vulnerabilities of the United States of America, v15*, provide extensive tactical guidance for sabotaging electric assets, instructions and calls for attacks on other critical lifeline sectors, extremist ideological narratives developed to radicalize individuals and justify violence, and other resources for potential assailants to seek out further information.

Although these documents contain tactics aimed at undermining the electric grid and other critical infrastructure, they are neither innovative nor sophisticated and do not provide a blueprint for bringing down an Interconnection or the bulk power system. Nevertheless, their availability does increase safety and security risks for industry.

This analysis was developed via coordination between subject matter experts from the Electricity, Health, Water, Downstream Natural Gas, Financial Services, Public Transportation, Over the Road Bus, and Surface Transportation Information Sharing and Analysis Centers (ISACs) in response to concerns expressed by members and stakeholders across multiple industries. It was developed to highlight the most concerning industry-specific tactics discussed in the publications and offer mitigation resources to help defend against the suggested attack methods (see **Appendix A**). The report enables sector stakeholders to navigate these documents and draws attention to the tactics and targets that coincide with some of the incidents observed across the different ISACs.

The ISAC partners are not currently aware of any credible threats to their industries related to the publication or resharing of extremist documents. However, the heightened threat environment facing critical infrastructure makes it essential for industry security practitioners to be aware of this information and monitor for threats related to the tactics described in the publications.

Sector stakeholders should refrain from referencing the documents or author(s) by name in public forums since extremist authors may monitor for online “mentions” and derive satisfaction and motivation from the notoriety; mentions may also inadvertently attract unwanted attention to a specific entity or its personnel.

Overview

Recent Publications

Redstone Killers (*RK*) is a 100-page extremist publication that was first observed on open-source archival sites and digital libraries and disseminated throughout anonymous online forums in early 2024.[1] The document promotes a variety of violent ideological perspectives and tactics, techniques, and procedures (TTPs) for sabotage along with their desired impacts and provides open-source media (e.g., diagrams, videos, maps, links) intended to guide self-radicalized lone-wolf or small-cell threat actors.

*The Known Vulnerabilities of the United States of America, v*15 (*TKV*), a 35-page document of a similar nature, was first observed to have been published online in 2021 and has been updated by the author(s) several times. The varying extremist beliefs observed within *RK* and *TKV* are best categorized under the U.S. FBI and Department of Homeland Security's (DHS) ideological terminology[2] of "All Other Domestic Terrorism Threats." The ideological basis is supported by accelerationist leanings with the desire to hasten societal collapse and includes opposition to economic, governmental, and social hierarchies due to perceived overreach.

Regarding the author or authors of the documents, "*Laserhawk*" is identified as the author on both documents' title pages. Multiple instances of "*Laserhawk*" asserting ownership of the publications have been observed online, yet—beyond this self-identification on various digital libraries and archival websites—additional information is scarce. However, given the diversity in writing styles and the presence of copied and pasted content, cross-sector ISAC analysts assess with low confidence that, although a single entity appears to be responsible for uploading the documents, both publications likely encompass contributions from multiple individuals.

RK and *TKV* represent the most recent extremist publications in the extremist media landscape. In comparison to previous publications, such as *The Hard Reset,* their organization and readability suffer from inadequate formatting and structural sophistication and fail to offer the same level of cultivated aesthetics.

The publications notably encourage readers to focus on attacking critical infrastructure rather than carry out mass-casualty violence, representing a shift from some of the previous publications. *TKV* reads, "Any terrorist group looking to cause undue harm to a nation should strictly attack infrastructure rather than the populace," underlining that mass-casualty attacks typically strengthen community ties while attacks disrupting infrastructure lead to resentment against the government and facilitate societal breakdown as people focus on their own basic needs. This highlights an acknowledgment by domestic violent extremists (DVE) and similarly motivated threat actors of electricity's pivotal role in society, positioning the electric grid and other critical "linchpin" systems as primary targets due to their foundational importance across all critical infrastructure sectors.

Previous Publications

Over the past several years, violent rhetoric and propaganda that encourages attacks against critical infrastructure has been shared across various digital platforms and accompanied by detailed instructions for using firearms to sabotage infrastructure, building explosives, operating drones, and undertaking other tactics. The period between June 2021 and July 2022 saw the publication of at least four documents

[1] See the E-ISAC Portal for a detailed analysis focused only on *RK.*

[2] *Domestic Terrorism: Definitions, Terminology, and Methodology*

commonly seen in extremist circles that encourage readers to attack electric and energy infrastructure along with the water and wastewater, transportation, communications, and healthcare sectors and a range of other critical infrastructure. These documents include *Militant Accelerationism*; *Do It for the 'Gram*; *Make It Count: A Guide for the 21st Century Accelerationist*; and *The Hard Reset.*

These publications promote various TTPs for attacking infrastructure assets, citing tools such as firearms; rudimentary improvised explosive devices; edged weapons; weaponized unmanned aerial systems (UAS); and tactics like arson, industrial sabotage, and assassination. For example, *The Hard Reset* includes 30 pages of tactical guidance for disabling critical infrastructure services based on accelerationist goals. The publication also details how to identify targets and choose tactics, describes asset vulnerabilities, provides operational security measures, outlines the desired impacts of violent attacks, and promulgates narratives meant to radicalize individuals to violence against specific types of critical infrastructure assets.

The documents in question espouse accelerationism, a belief held by some extremists suggesting that the existing state of society is irreparable and that the only solution is the destruction or collapse of the social order. Violent extremists who subscribe to accelerationism believe that violent action is necessary to accelerate the impending societal collapse, and often advocate for social disruption through violence on critical infrastructure. Some believe such action will lead to large-scale conflict in Western democracies, often framed as a race war or civil war that will result in a white ethnostate. Adherents to this philosophy represent widely varying ideologies yet may share similar grievances, thus inviting promotion of accelerationist ideas focused on destabilizing existing societal systems and attacks on infrastructure.[3]

A number of threats, plots, and attacks may have been influenced by the release of these violent extremist publications. For example, the violent extremist who shot and killed multiple people at a bar in Europe in October 2022[4] cited *Militant Accelerationism* and *The Hard Reset* as recommended reading in his 65-page manifesto. He also directed readers to "target infrastructure; destroy necessary utilities…electricity, water supply, sanitation, fiber-optic cables, cell towers." This highlights the potential influence of these documents to radicalize individuals and provide them with information and perceived justification for mobilizing against infrastructure. Convicted DVEs have also cited the publications' tactical insights in sharing and recommending them to other extremists. For instance, convicted DVE Brandon Russell, who was arrested last year for conspiring to attack the power grid[5] in Baltimore, allegedly shared the DVE publication,[6] *Make it Count: A Guide for the 21st Century Accelerationist* with other would-be attackers and told them to study it.

Ideological Background

RK and *TKV* promote a wide variety of extremist beliefs, including anti-Semitic, white supremacist, misogynistic, and anti-government ideas. Given the presence of varying extremist beliefs—along with conspiracy theories, reverence of multiple figures, and a lack of a coherent ideology displayed—these documents are best reflected under the DHS's ideological category of "All Other Domestic Terrorism

[3] See Volume 4, Issue 10 of the CTC Sentinel.
[4] https://www.hstoday.us/featured/slovak-who-attacked-gay-bar-credits-buffalo-shooter-with-giving-him-final-nudge/
[5] https://apnews.com/article/politics-crime-maryland-baltimore-1b193a88f54001a882691f2c5da37f11
[6] https://www.splcenter.org/hatewatch/2023/02/23/leaked-chats-documents-show-atomwaffen-founders-path-terror-plot

Threats."[7] The DHS's definition states that this category can include beliefs derived from sources including "a mixture of personal grievances and beliefs, political concerns, and aspects of conspiracy theories, including those described in the other [domestic terrorism] threat categories." The definition adds, "Some actors in this category may also carry bias related to religion, gender, or sexual orientation."[8]

Despite the lack of a coherent ideological narrative, the author(s) clearly reject non-violent action and instead promote violence against electric infrastructure to achieve their goals. The documents espouse the concept of accelerationism, which, while ideologically agnostic, calls for violence against infrastructure and government targets to hasten the establishment of a new socio-political order. These types of ideas are often espoused by both RMVEs and AGAAVEs. Rife with racial and ethnic slurs, many of which are directed toward Black and Jewish people, the writings advance conspiracy theories as a justification for violence, including well-known anti-Semitic conspiracy theories claiming that Jewish people control the U.S. government and Holocaust denial.

At multiple points, *RK* describes electric infrastructure as a central tool used by the fictitious Jewish cabal to control the United States. Various racial minorities, along with mixed-race individuals, are also mentioned. In *TKV*, the author(s) posit that a portion of Black and mixed-race people in the United States should be killed, adding the call to action that "if Amerca will not comply, it should be overthrown in a race war…" The documents include many graphic depictions of violence against women,[9] including promoting violence against a substation power transformer to enable sexual assault. The author(s) also glorify extremist individuals/groups in the documents. For example, in *TKV*, white supremacist attackers, including Anders Breivik, Dylann Roof, and Brenton Tarrant, are praised along with other figures including Kim Jong Un, Mohammed bin Salman, and the Washington, D.C.-area snipers.

In line with the common accelerationist practice of gamifying violence to appeal to juveniles and adolescents, both documents reference the video game *Minecraft*, which is also referenced in *The Hard Reset*. *RK* specifically uses the idea of a "redstone," an item from Minecraft, to articulate its argument. It is likely that "redstone," in the context of *RK*, symbolizes the electric industry; in *Minecraft*, redstone is used to craft items and infrastructure related to electricity.

[7] The DHS breaks domestic terrorism ideologies down into five categories: Racially or Ethnically Motivated Violent Extremism (RMVE), Anti-Government or Anti-Authority Violent Extremism (AGAAVE), Animal Rights/Environmental Violent Extremism, Abortion-Related Violent Extremism, and All Other Domestic Terrorism Threats.

[8] *Domestic Terrorism: Definitions, Terminology, and Methodology*

[9] For example, see *RK,* page 32.

Cross-Sector Concerns

The concept of weaponizing electricity to enhance negative impacts on other sectors is the commonality between most DVE narratives that promote attacks on critical infrastructure; this is also true with *RK* and *TKV*, which provide multiple tactics for attacking electric sector assets in order to impact other critical sectors. This section highlights the different types of cyber and physical attack tactics promoted, including the use of malware against IT/OT systems. Tactical guidance for law enforcement evasion and tips for operational security measures are also discussed.

Blended Cyber and Physical Threats

Some of the capabilities and tactics discussed in *TKV* represent a blended threat that could be applicable across the critical infrastructure sectors relying heavily on cyber-physical components, systems, and technologies. Risk-management firm Gate 15 defines a blended threat as a "natural, accidental, or purposeful physical or cyber danger that has or indicates the potential to have crossover impacts and harm life, information, operations, the environment, and/or property."[10]

For example, an insider cyber threat actor could use the encryption script provided in *TKV* to disrupt operations at a utility or other organization given their pre-existing access to critical systems. Additionally, a physical threat actor could affect blended systems through tactics such as intrusion and tampering by breaching an organization's facilities to gain access to and manipulate its incident command systems (ICS). Technically proficient individuals, for example, could use the information in the documents to acquire or construct an intentional electromagnetic interference (IEMI) device, such as a radio frequency (RF) suitcase, to disrupt infrastructure operations with what is effectively a small electromagnetic pulse (EMP) attack.

Physical security devices are often digitally connected through devices such as electronic locks and security cameras, creating risks for organizations with weak cybersecurity programs in place. Cyber-physical attacks represent a unique and concerning category as they aim to exploit vulnerabilities in both the digital and physical domains simultaneously, sometimes resulting in blended impacts. By targeting interconnected digital and physical systems, these attacks pose an elevated risk and can result in significant operational disruptions, financial losses, and the compromise of sensitive data or physical safety.

TKV notably calls for readers to conduct cyber attacks on infrastructure organizations, providing guidance for locating infrastructure assets in the physical and cyber domains. In *TKV*, the author(s) list four "Vulnerable American SCADA VNC Servers" said to be associated with critical infrastructure systems in the United States and identify respective IP addresses. The document also includes what it describes as a "PYTHON CYBERWEAPON CONCEPT" that provides code for three different encryption viruses as well as another script described as a "POLYMORPHIC ENCRYPTION VIRUS," with the author(s) claiming that the code is for "true encryption malware" and stating that "chaos occurs when governments and infrastructure lose absolutely everything."

According to an E-ISAC analysis, the statements are very generic, seemingly intended to be called on or used with other scripts or malware. It appears that the code may be used for staging data internal to a victim network by setting up encrypted channels to aggregate it in one spot on the file system before data exfiltration. To avoid security defenses triggered by multiple requests to transfer files from various parts of

[10] https://gate15.global/blended-threats-understanding-an-evolving-threat-environment/

a file system, threat actors typically stage data before exfiltrating to allow them to export one packaged bundle. WaterISAC's operational technology (OT) advisor also noted that the polymorphic encryption script is missing crucial parts, making it ineffective for use as written.

Despite the likely generic and ineffective scripts included in the publication, this section of *TKV* displays how extremists who are usually engaged with physical attack tactics are increasingly interested in and inspired by cyber attack methods. The use of cyber weapons, starting with Stuxnet in 2010[11] and spreading to Ukraine in 2015, 2016, and 2022, shows how effective a cyber attack against critical infrastructure can be. In 2022, Russian actors used wiper malware against satellite communications networks supporting Ukrainian defenses. Outside of impacting critical infrastructure in Ukraine, the "Acid Rain" used in this attack inflicted collateral damage on German wind-turbine manufacturer Enercon, causing it to lose its satellite-enabled connection to 5,800 turbines.[12] While no electric customer outages resulted from the attack, Enercon was forced to invest substantial resources to replace the satellite modems.

Other types of malware, such as ransomware, are proven weapons within the tradecraft used by cyber threat actors wishing to act against critical infrastructure sectors. According to data from the FBI's Internet Crime Complaint Center (IC3), ransomware incidents against critical infrastructure entities have increased in recent years, rising from 649 total reported incidents in 2021 to 1,193 in 2023. While no reported ransomware attacks have caused electric customer outages to date, the 2021 ransomware attack against the Colonial Pipeline, which transports motor and jet fuel, is an object lesson in how a ransomware attack could impact the delivery of critical infrastructure. The attack inside the pipeline's information technology system resulted in the pipeline's operations being shut down, causing the perception of a gasoline shortage and a resulting "panic buying" spree on the East Coast.[13] The E-ISAC has recently observed an increase in ransomware incidents in Q1 2024 in comparison to Q1 2023.[14] This increase in ransomware incidents against critical infrastructure illustrates the disruptive effects[15] that encryption-based malware can have on an organization's ability to operate.

Although there are opportunities for the information shared in *TKV* to be leveraged by a skilled actor in a cyber attack affecting critical infrastructure sectors, this information is not unique from a cyber perspective. The author(s) share publicly available open-source tools, Darknet email services, python code, and IP information relating to a substation, but none of these pose a substantial risk to the electric sector or other critical infrastructure sectors beyond commonly accessible threat vectors. The E-ISAC assesses with medium confidence that *TKV* provides little to no actionable information and that the author(s) are not technically inclined from a networking standpoint. This assessment is based on the mischaracterization of a substation IP address, which was verified through Shodan as not being associated with an electric substation in addition to being registered in a different state than mentioned by the author(s).

The author(s) seem motivated from a threat characterization standpoint, but their lack of underlying capabilities and skills required to initiate an attack suggests that violent action is unlikely, whether in the

[11] Alvarez, Joshua, "Stuxnet: The world's first cyber weapon," Stanford University's Center for International Security and Cooperation
[12] Guerrero-Saad, Juan Andres and Max van Amerongen, "Acid Rain | A Modem Wiper Rains Down on Europe," Sentinel Labs, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
[13] U.S. Department of Energy, Colonial Pipeline Cyber Incident, https://www.energy.gov/ceser/colonial-pipeline-cyber-incident
[14] See annual review for January, February, and March 2023 monthly ransomware incidents. See monthly OSINT reports for January, February, and March 2024 monthly ransomware incidents.
[15] https://www.techtarget.com/searchsecurity/news/366570061/Ransomware-disrupts-utilities-infrastructure-in-January

electric sector or the other lifeline sectors. Furthermore, the cyber tools and tactics shared are commonly available and require substantial development of further skills and capabilities to cause significant harm to any of the critical lifeline sectors. Individuals with the capability to do so are unlikely to benefit from the sharing of these open-source tools, of which they would most likely be already aware.

Operational Security Measures

Both *TKV* and *RK* contain several suggested operational security measures to aid in violent action and avoid detection by authorities. For example, *RK* highlights several perceived operational security failures in the Metcalf and Moore County, North Carolina substation attacks. The author(s) write, "To avoid a repeat of the failures of Metcalf and Moore County, I have outlined what you need to do, step by step, based on common sense"[16] and provide a list of suggested steps, including those below, to ensure a successful attack against the grid:

- Leaving smartphones and other technology at home
- Covering head-to-toe in black clothing, including gloves, boots, and balaclavas
- Using paper maps and atlases
- Calling in a credible threat to a nearby location to draw police away from a planned target

In addition, a section in *RK* directly leverages information from another document, *Gridnomicon,* which provides comprehensive operational security guidance for small-group violent action. This section offers several additional recommendations to evade detection and hinder investigators, including the following:

- Using two different vehicles—one stolen, one not—for travel
- Using stolen cell phones for communication
- Having two changes of clothing for the attack, including one all black and one casual outfit
- Wearing rubber gloves for touching electronic equipment
- Wearing ear protection, clear goggles, and gloves if conducting a ballistic attack
- Utilizing a "brass catcher" to catch shell casings

TKV also provides similar recommendations to facilitate a violent attack, including advising would-be attackers that the Fourth of July and New Year's Eve are ideal times to carry out ballistic attacks as fireworks can mask the sound of gunfire and make shootings more difficult to detect. *TKV* advises targeting electric infrastructure between 11:00 p.m. and 2:00 a.m. as "the cops will be tired and there will be a shift change around 3 - 4am. You want tired hungry cops. Not freshly awake cops who just ate."

TKV also touches on operational security measures for using the internet and online platforms, suggesting that, when going out to commit a crime, threat actors should leave their phone at home playing an automated playlist of YouTube videos to give the appearance that they were home watching online content. Additionally, *TKV* discusses manifestos, livestreams, and developing violent propaganda along with the

[16] *RK*, page 35.

importance of minimizing identifiable information. For example, the author(s) stress that threat actors should not "let an empty bag of chips or a water bottle get you [messed] up," adding, "DO NOT have anything regional or any brand or label based [stuff] on you or on the ground or in your location, don't show any markings, tattoos, scars, don't speak unless you can scramble your voice, [as] you may have a regional accent or set of slang words."

The author(s) urge against livestreaming attacks because doing so can disclose a wealth of identifiable information and state that those willing to make "real" and "noticeable" change will not livestream. For example, the authors describe mass shooter Brenton Tarrant as "ignorant" for streaming his Christchurch mosque attack but express admiration for serial killers such as Ted Bundy for being able to "kill for years" by maintaining anonymity. In summary, the range of operational security recommendations provided in *RK* and *TKV* demonstrates that the author(s) have invested a notable amount of time into attempting to understand violent action, particularly against critical infrastructure.

Analysis of Infrastructure Interdependencies and Impacts

Overview

Power outages caused by attacks on electric infrastructure have the potential to strain or disrupt other critical infrastructure sectors and can result in significant loss of life. For example, a July 2022 attack on an electric substation in South Dakota caused power outages and cascading impacts to the Keystone Pipeline.[17] Given that nearly all other critical infrastructure sectors depend on electricity for operation, a comprehensive understanding of the threat landscape facing the electric industry is of high importance. This knowledge enables infrastructure owners and operators to effectively mitigate and prepare for potential power disruptions.

The following sections analyze impacts created by loss of power for each of the following lifeline sectors: downstream natural gas, transportation, water and wastewater systems, healthcare, and financial services.

Natural Gas

Degradation, disruption, and destruction of natural gas distribution and transmission pose significant cascading challenges to critical infrastructure, impacting sectors ranging from electric generation to water treatment and industrial processes. These challenges include the following:

Natural gas-fired power plants have been a major contributor to electric generation in the United States. The U.S. Energy Information Administration (EIA) identified the total electric generation capacity from natural gas in the U.S. as approximately 500 GW as of 2020. Natural gas generation also provides unique dispatchable power that is difficult to replace with other generation sources such as coal, which has a long ramp-up time, and renewables, which are not dispatchable unless combined with grid-scale energy storage. The potential direct consequences of loss of natural gas include blackouts and cascading disruptions to other critical infrastructure sectors.

As residential and commercial buildings rely heavily on natural gas for heating and cooking, a loss of supply would disrupt daily activities, emphasizing the importance of a stable energy supply for society.

Natural gas plays a pivotal role in powering water treatment plants, encompassing vital components such as pumps and heaters. A disruption in supply could compromise water supply, sanitation, and public health, underscoring the interconnectedness of natural gas distribution and public welfare.

Industries rely heavily on natural gas for processes like heating, drying, and chemical production. Disruptions in natural gas supply would significantly impact manufacturing operations and global supply chains.

Transportation

If catastrophic failure of the power grid occurred in the United States, regardless of circumstance, most public transportation would struggle to operate. The transportation sector is one of the lifelines of modern society. It is critical to ensuring the accessibility of goods and services and moving people to and from work and places of interest. Furthermore, various aspects of transportation, such as mass rapid transit (MRT), locomotives, and the rapidly transitioning electric bus and vehicle fleets, are deeply interconnected with that of the electric sector.

[17] For more detail see E-ISAC Portal at TLP:AMBER Article ID 000014755.

In November 2022, a single-engine private plane crashed into a transmission line in Montgomery County, Maryland.[18] Although emergency responders quickly resolved the incident, the crash significantly disrupted the operations of the Washington Area Metropolitan Area Transit Authority (WMATA) and Maryland Transit Administration (MTA) by knocking the WMATA red line out of service and delaying the MTA Brunswick Line trains by 20–30 minutes as the outage "resulted in interruptions to CSX signals and switching equipment, causing trains to significantly reduce speeds."[19] MRT trains and locomotives are controlled electronically by central dispatch centers, switching equipment, and Positive Train Control (PTC), meaning that, if connectivity is lost, public transit ceases to be safe or functional. This uncontrollable event illustrates some of the repercussions that transit would suffer if DVEs successfully attacked the power grid.

Water

Power outages can significantly impact water and wastewater utilities and the communities that they serve. Inoperable pumps at utilities can halt the treatment of drinking water and wastewater, make firefighting difficult, and cause hospitals and businesses to close. Pressure loss can allow harmful contaminants to enter the drinking water distribution system from surrounding soil and groundwater. Power outages can also result in cascading impacts to critical infrastructure and losses of critical lifeline services for the water and wastewater sector. For instance, a disruption of power would almost certainly knock out telecommunication services, obstructing a utility's ability to communicate with its personnel and other key stakeholders. In another example, a disruption of power would most likely impact the chemical and transportation sectors, which could in turn affect the manufacturing and shipment of chemicals that water and wastewater utilities rely upon for treatment operations. The loss of power could have direct impacts on wastewater utilities, preventing them from processing wastewater, causing the system to back up and potentially leading to the discharge of untreated sewage directly into communities.

Due to the power grid's interdependency with the water sector, attacks that disrupt the grid would certainly produce cascading impacts to operations and services for water and wastewater utilities. One notable case occurred in December 2022 when an unknown individual or group attacked two electric substations in central North Carolina, using firearms to substantially damage equipment and causing approximately 45,000 customers to lose power.[20] The power outages led to cascading impacts to multiple critical infrastructure sectors, including the water and wastewater systems. In one small town, water and sewer services were forced to run on backup generators,[21] disrupting operations until the utility could bring backup generators online.

Health

Most patient-facing healthcare facilities, such as hospitals, have backup generators that ensure continuity of operations in the event of a power outage. However, delays in backup generator startup could cause life-supporting systems to power down, which disrupt these systems if their startup is delayed. Power loss could also impact healthcare workers' ability to perform procedures, properly sterilize equipment, and preserve

[18] https://www.washingtonpost.com/dc-md-va/2022/11/27/plane-crash-power-lines-montgomery/
[19] https://www.mta.maryland.gov/service-alerts/12995

[20] See TLP:AMBER Article ID 000015575 and TLP:GREEN Article ID 000015618
[21] https://www.fayobserver.com/story/news/crime/2022/12/04/moore-county-power-outage-investigated-as-vandalism/69699328007/

medications. Generators providing uninterruptible power supplies will generally run a portion of the load required by a hospital, limited only to the most critical sections, such as emergency departments. In the case of longer-term blackouts, manufacturing can also be disrupted, delaying the ability to produce medications or medical devices and potentially causing a severe delay in supply chains by delaying further production or ruining previous productions, such as those supported by refrigerated medications. Although contingencies exist within the healthcare sector to protect patients and staff during a power outage, a longer-term outage could cause an increase in loss of life and result in disruptions that lead to a lengthy recovery.

Financial Services

Absent any significant change in the current threat environment, critical infrastructure sectors will likely remain a focus of documents composed by DVEs who continue espousing violent rhetoric against critical infrastructure. These threat actors' primary objective is to disrupt the grid to cause cascading impacts, exploiting interdependencies of other critical infrastructure sectors in the hopes that these attacks will motivate other likeminded individuals to violence with the aspirational goal of overthrowing the existing political order. *RK* and *TKV* include explosives-manufacturing instructions and list targets for attacks that would accelerate the destruction of the political order by impacting multiple sectors, illustrating this objective in a number of ways. Overall, the weaponization of electricity as a means to attack financial services institutions is a proven tactic[22] and a concern for the sector.

[22] https://www.justice.gov/usao-wdwa/pr/first-two-defendants-sentenced-prison-christmas-day-2022-attack-power-substations

Sector-Specific Tactics and Concerns

Overview

RK and *TKV* primarily focus on providing tactical guidance for sabotage against the electric grid more so than against other types of infrastructure. As mentioned previously, the author(s) of these extremist publications recognize the first-line importance of electricity as an enabling function of society and therefore aim to compound effects on these functions by focusing attacks on grid assets. The TTPs and weapons described in the two documents are nearly identical at a high level, though the approaches, levels of specificity, and usability of the information vary widely. For example, while *RK* provides more technical information, such as detailed instructions and diagrams, it is largely devoid of context and is a non-homogeneous composition of different media types and styles. Conversely, *TKV* provides a consistently succinct approach when describing attack tactics and contains a wide range of notes written by the author(s) meant to provide only the most essential outline of tactics and procedures with further recommendations for reading or viewing to provide contextual understanding of grid assets and components for the purpose of violent action. Both documents also advocate for the use of different types of weapons that can be applied broadly, including explosives, electromagnetic pulses, radio jammers, and firearms.

Electric Sector

The tactical guidance provided in the publications is supported by highly detailed technical diagrams of substation power transformers, multiple forms of detailed guidance for the development of explosives, and specific instructions providing lessons learned and techniques for avoiding detection for varying levels of evasion. The guidance provided leverages a variety of open-source materials, including blog posts, online encyclopedias, government websites, open-source maps and infrastructure datasets, and news articles.

Tactics

This section discusses the tactics described for use against the electric sector in *RK* and *TKV* in comparison with certain tactics involved in grid-impacting incidents[23] shared with the E-ISAC. More information regarding the frequency of grid-impacting incidents and the respective tactics involved is provided in the E-ISAC report on physical security incidents affecting the electric sector[24] and the quarterly incident reports posted regularly on the Portal.

The tactics most frequently discussed throughout *RK* and *TKV* include the following:

- **Ballistic damage** to target a variety of specific components of a substation power transformer
- **Vandalism**, including the use of Mylar ballons on distribution conductors, arson of power transformers, and felling of lattice transmission structures.

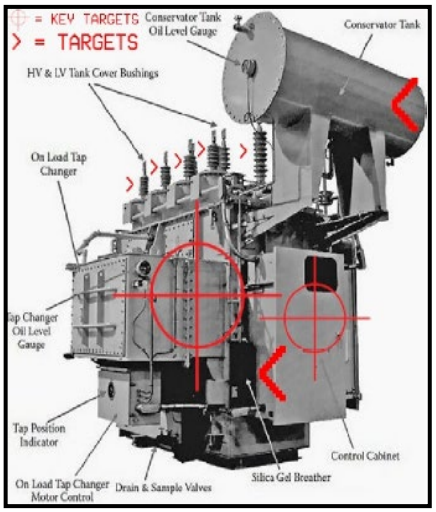

Figure 1: "Where are the key points to hit on a transformer" *RK*, p. 12

[23] See the E-ISAC Physical Security Incident Methodology: Severity Level Framework
[24] See the E-ISAC Physical Security Report: Grid-Impacting Incidents (2022-2023)

Although these tactics have been observed in grid-impacting incidents, the E-ISAC assesses with high confidence that none of the tactics described in *RK* or *TKV* can produce cascading failures to the electric grid. Regardless, one notable example of promoted tactics (targeted ballistic attacks against substation power transformers) is shown in **Figure 1**. Although this tactical information is not original and already available in a plethora of resources on the clear web, including resources that are not extremist in nature, the threat of ballistic attacks against substation power transformers provides credible and concerning capabilities that have previously led to operational disruptions, such as with the Moore County substation attacks.

As it pertains to incidents involving vandalism, only a small percentage of the tactics discussed in both publications has been observed in the incidents shared with the E-ISAC. For example, there have been no incidents shared with the E-ISAC involving the use of arson to target substation power transformers, although other assets have been affected by this tactic. While relatively infrequent[19], another tactical subtype of vandalism described in the two publications is malicious felling, which involves the deliberate cutting down of trees, distribution poles, or transmission structures to disrupt service. Lastly, the use of Mylar balloons on energized equipment (which the E-ISAC categorizes as vandalism/airborne object) is also discussed in *RK* and *TKV*, but there have only been two incidents involving the targeted use of Mylar balloons shared with the E-ISAC since 2020 even though this tactic is frequently cited online as a way to disrupt power. Although this could be due to sharing biases, with asset owners and operators (AOO) assuming that such incidents are accidental, the E-ISAC also assesses that, as Mylar balloons are likely very difficult to control in a precisely targeted manner, motivated actors are more likely to select other, more controllable techniques for sabotage.

Additional examples of tactics discussed the publications that have not yet been observed by the E-ISAC include the following:

- Suspicious use of UASs used to drop graphite powder on substation power transformers
- Detonation of ammonium nitrate–fuel oil (ANFO) explosives, improvised explosive devices (IEDs), potassium chlorate cluster bombs, and Tannerite™ near substation power transformers, in addition to other explosives

Tannerite™ is the trademarked brand name of a readily available improvised energetic material (IEM) that, according to Balachandar and Thangamani (2019),[25] is used by "Irish, Spanish, Chechen, Saudi Arabian and Kashmir terrorists." It is less potent than TNT but has low detonation thresholds for temperature, velocity, and pressure relative to other IEMs, allowing it to be detonated by rudimentary means, such as high-caliber/powder gunshot. Tannerite™ can be purchased in many parts of the United States from hardware stores without a background check or any other control. Even so, Tannerite™ is unlikely to be to successfully target substation power transformers due to the numerous logistical hurdles that it introduces. In fact, individuals entering substations and coming close enough to energized equipment to place minor explosives can, before even placing the device to be detonated, expect life-threatening conditions and face likely fatal

[25] (Balachandar and Thangamani, 2019). Studies on some of the Improvised Energetic Materials (IEMSs): Detonation, Blast Impulse and TNT Equivalence Parameters. *Oriental Journal of Chemistry*. 2019, Vol. 35, No. (6). https://pdfs.semanticscholar.org/70f9/98bc3647bb9cd95b7475d7daba179f71adcd.pdf

wounding, rendering them potentially unrecoverable, if they come into contact with energized equipment due to the high degree of electricity and heat produced. ANFO explosives and potassium chlorate cluster bombs are both realistic homemade explosive compositions that have been previously used by terrorists[26] but require some sophistication and dedication in their development. Cluster munitions, however, are not likely to be employed by DVE threat actors without a significant source of funds.

According to Jeler and Roman (2016),[27] the effective use of a graphite bomb to circumvent the existing redundancies and disable an electric system requires "a detailed knowledge of the system architecture…with a correct identification of its critical points" followed by a large-scale attack using hundreds of graphite canisters, a "massive use of graphite," at each attack point. Furthermore, the components utilized inside of the graphite bomb are highly complex and not easily manufactured in a non-industrial environment. Therefore, the E-ISAC assesses that the author(s) demonstrate a lack of understanding of critical infrastructure and the built environment by promoting ineffective sabotage techniques.

Table 1: Summary of TTPs in *RK* and *TKV*—Tactics and Assets

		Asset Type and Subtype Mentioned in Documents				
		Substation/ Power Transformer	**Transmission/ Structure**	**Distribution/ Conductor**	**Communications/ Fiber** (Supporting Electricity Comms)	**Other** (Utility Personnel)
Incident Type and Subtype	**Ballistic Damage**	x				
	Vandalism					
	Detonation	x				
	Airborne Object (Mylar Balloons)			x		
	Arson	x				
	Cut Wires				x	
	Felling		x			
	Suspicious Activity					
	UAS	*x*				
	Other				*x*	
	Surveillance					
	Reconnaissance	*x*				
	Assault					*x*

[26] (Horrocks, et al., 2023). Chlorate-based homemade explosives: A review. https://doi.org/10.1002/wfs2.1506

[27] (Jeler and Roman, 2016). The Graphite Bomb: An Overview of its Basic Military Applications. *Review of the Air Force Academy.* No. 1 (31) 2016.

In addition to descriptions of specific attack tactics, both documents describe asset and systemic vulnerabilities, evasive techniques to be used during and following attacks on electric infrastructure, and lessons learned from previous attacks, which are exceedingly unsophisticated in their analysis.

E-ISAC Assessment: Overall, the E-ISAC assesses with high confidence that the degree of impacts that the author(s) of these publications envision—systemic collapse and cascading impacts or power grid failure—are highly unlikely through the means described due to the systemic reliability and resilience of the North American electric grid. Even so, the tactics promoted do illustrate the potential risk to the electric industry in terms of monetary losses and operational disruptions resulting from such incidents. The impacts on adjacent sectors may be palpable but are unlikely to be extreme or critical on a large scale.

Water Sector

RK and *TKV* are the latest in a continuing series of violent extremist publications calling for attacks on water and wastewater systems and other critical infrastructure sectors as a means of sowing chaos and fomenting the overthrow of the existing socio-politico order. Both documents discuss a number of TTPs for targeting the water and wastewater sector. As some of the suggested tactics require advanced technical skills, successfully conducting these attacks would likely be difficult for the average individual.

Among the TTPs, the two documents recommend dumping chemical or biological agents into a drinking water supply. In *RK*, for instance, the author(s) write that attackers could "throw cutaneous anthrax or bubonic plague laden severed arms and legs into a water tower. Or 200 pounds of fentanyl. Or [f**k] ton polonium. Or dimethylmercury." WaterISAC has tracked past incidents involving break-ins at water storage sites, some of which went undetected for days, demonstrating that attackers could potentially access critical points in storage facilities to contaminate or disrupt water supplies.

Nevertheless, a number of factors, such as the layout of the system pipes, dose of the agent, and method of introducing the agent, would impact the distribution and effects of a water contamination attempt. The first sign of such an attack may appear as a cluster of illnesses reported to public health officials. Such an attack could promote fear and panic in the community even if a contamination attempt did not achieve massive health effects. The uncertainty associated with the lethal doses and persistence of many chemical and biological agents in drinking water could increase public fear.

Still, gaining access to the chemicals and biological agents and the significant care needed to handle the material would likely impede an attacker's ability to contaminate water supplies. Fentanyl, however, is readily available on the black market. The drug is also extremely potent, and it would likely only take the introduction of a small amount of it into a distribution system to significantly impact public health, according to a subject matter expert in hydrology at the National Research Council of Canada.

The documents recommend other additional TTPs for targeting water and wastewater systems, but these are more technically advanced and operationally complex. *TKV* offers guidance for a "Superweapon Concept" to conduct a radiological attack in the air or water supply using multi-layered effervescence radiological dispersion devices (MLERD). It also describes how to make and use "Radioactive Graphite Nanoparticles Within Microparticle Lead Spheroids with Elemental Sodium/Aluminum/Iron Oxide Shell, Hygric Trigger" to make various MLERD explosive devices and munitions. The document additionally discusses how to weaponize and employ UASs, or drones. For example, the author(s) recommend attaching

a spraying device to a drone to conduct attacks using various chemicals with devices such as a "Dimethylmercury Spraying Drone."

Lastly, the author(s) provide information on targeting an infrastructure organization's industrial control systems using a non-nuclear EMP attack. The document provides links for requisitioning or creating an RF suitcase to execute an EMP attack. The probability of a threat actor successfully constructing these devices and deploying them in a source of water or against a water utility is likely low. However, the recommended tactics still offer aspirational means of sabotaging water and wastewater systems, which could motivate other potential threat actors to design other novel sabotage methods.

WaterISAC Assessment: WaterISAC assesses that the TTPs advocated in these documents, coupled with other tactics encouraged in previous DVE publications, likely increase the risk of sabotage against the water and wastewater sector because the documents highlight sector vulnerabilities, potentially increasing the perceived viability of the sector as a target. WaterISAC also assessed in its 2023 Threat Analysis Report[28] that individuals or groups that embrace accelerationism are the most likely and lethal physical threat of extremist targeted violence against the water and wastewater sector. Since the extremist documents under discussion promote accelerationism and the targeting of water infrastructure, the 2023 assessment remains valid. Due to the heightened threat environment facing critical infrastructure,[29] water and wastewater utilities are encouraged to consider the potential attack methods outlined in the documents to reassess their security posture and determine steps to mitigate potential vulnerabilities.

Transportation Sector

TKV highlights various ways that a DVE can exploit and target the transportation sector to pursue the collapse of American society. In particular, the publication encourages readers to utilize public transportation, namely MRT, when traveling to and from planned attacks against critical infrastructure and politicians because riders can retain a certain amount of anonymity when using surface-based public transportation. The author(s) advise the reader to "use Greyhound because they don't ask much or hop…trains" after an attack. The Public Transportation, Over the Road Bus, and Surface Transportation ISACs assess this technique to be of low to mid concern. Subway surfing and train hopping are extremely dangerous and often end with the "surfer" dead or severely injured. Additionally, the author(s) fail to take into consideration how a surfer would transport heavy and bulky military-grade weapons needed for a critical infrastructure attack while train hopping. Although the publication recommends learning how to train surf with an experienced hopper, the likelihood of being caught is also extremely high. In 2023, the Metropolitan Transportation Authority of New York documented over 450 instances of subway surfing in six months, with 88 of those instances ending in arrests. New York Governor Kathy Hochul increased the number of police officers in stations on elevated lines to combat the trend, and, as the dangerous trend gains interest, public transportation organizations have added additional security cameras and sensors to detect individuals riding outside of trains.

[28] See WaterISAC 2023 Threat Analysis Report

[29] See Department of Homeland Security Homeland Threat Assessment 2024, Executive Summary and section on Critical Infrastructure Security.

The publications make further tactical recommendations of derailing trains and hijacking modes of transportation carrying explosives, weapons, and food. DVEs have long called for derailing trains and disrupting the supply chain when advising other extremists on how to cripple society. As stated earlier, transportation is the lifeline of modern society, and extremists aim to exploit the sector by targeting its infrastructure, such as bridges, tracks, roads, and highways. The author(s) write: "Police will show up to derailments when the area has roads. You derail a train in a city, cops come…If you derail a train, do it on a bridge crossing over water or do it in the middle of nowhere. Police response will be limited…" The strategy of derailing trains to incite chaos is of great concern to the transportation sector, as all derailments can pose a serious safety risk and disrupt future rail operations. Derailments clog railway infrastructure and force other trains to either be delayed, rerouted, or completely halted. The extremist documents also suggest that extremists "steal trains to block roads and bridges." The Public Transportation, Surface Transportation, and Over the Road Bus ISACs assess that blocking roads is a mid-to-high-level tactic of concern for the transportation sector, as prolonged roadblocks threaten the safety of drivers and their passengers and even shorter roadblocks also prevent first responders from responding to emergency calls. A 2017 study[30] found that death rates for elderly patients with major cardiac emergencies were higher on days with road closures in major cities, with the increase in death rates attributed to ambulances facing delays in getting to the hospital. The study found that road closures lengthened ambulance rides by 32%. If roads were blocked for an extended time, the effects of the blockage would likely be amplified as drivers would eventually abandon their vehicles, further impeding traffic. The U.S. highway transportation system supports 86% of all personal travel, 80% of freight, and the mobility of national defense. In the case of a severe, extended road blockage, loss of life and economic disruption would likely result.

Transportation Sector Assessment: The tactics provided in *TKV* intended to disrupt the transportation sector are unsophisticated and typical for extremist rhetoric calling for the sabotage of transportation infrastructure. The recommendations are more theoretical than practical, as it would likely take a group of highly trained individuals to successfully conduct an attack destructive enough for sustained or widespread failure.

Healthcare Sector

Although healthcare is not a primary target in *TKV*, it is mentioned four times as a potential target in an attacker's larger operational goals, as follows:

- The first mention is in reference to strategies for escaping prison. The author(s) state that it is near impossible to escape modern prisons, but, if granted the opportunity to visit an offsite hospital, an inmate could escape under the reduced security conditions. The author(s) posit that most successful prison escapes are from hospitals.
- The second mention is in describing the horrors that the author(s) anticipate in the event of a civil war, with the failure of the power grid causing life-support machines to shut down and family members to die. The passage references an RF suitcase (a tool discussed later in the document) as being useful in disrupting electric infrastructure specifically in hospital settings.

[30] https://www.nejm.org/doi/full/10.1056/nejmsa1614073

- The third mention is included in the author(s)' listing of the operational failures of the perpetrator(s) of the 2015 Metcalf Substation attack. The author(s) state that the attacker(s) should have made a false bomb threat to a local hospital or airport to draw police away. The author(s)' recommendations seem to show a lack of understanding in what happened in the attack they are referencing because most of the recommendations are irrelevant to what occurred. The recommendation to make a bomb threat is meant to prevent police from intervening in the attack even though in the Metcalf PG&E attack the police failed to stop the attack or catch the attacker. The author(s) were likely looking for an opportunity to recommend a bomb threat.
- The fourth mention is in reference to using an RF suitcase, a device that replicates the effects of an EMP and is used to test system resiliency. The document states that an RF suitcase could be used to shut down life support in a hospital setting or other forms of infrastructure that operate using electricity. There are some repeated themes in the writing, but mentioning healthcare in a threatening tone is usually used to antagonize the reader.

Healthcare Sector Assessment: The document only specifically mentions targeting a hospital setting once, namely in threatening lives with an EMP device with the intent of shutting down life-supporting equipment. The other mentions are means to an end that involve other topics, including escaping from prison, collateral damage from warfare, and a bomb threat as a distraction. Healthcare falls within the accelerationist aim of collapsing infrastructure and causing mass panic to reinvent society, though there is arguably a moral restriction if not a logical one in that society needs healthcare regardless of cultural disagreements. The threat to healthcare is existent but is assessed to be only in a collateral sense. Should the extremist goal be met on a large scale, then healthcare would be at risk, but the industry is not typically a direct target.

Financial Services Sector

RK specifically calls out financial institutions as targets for attack. The author(s) state that direct action against the financial sector (with the dollar sign ($) symbol) will create economic hardships that will in turn result in the destruction of the current domestic political system. For example, *RK* shows a graphic of large hands holding bags of money to illustrate a "lemming" state that needs to be disrupted by direct action against the "system," including those involved in distributing money. The remainder of the document is mostly devoted to instructions on how to attack the electric sector with the explicit purpose of creating cascading impacts that will disrupt and shut down other key critical infrastructure sectors, including the financial sector. In another concerning example, *RK* recommends the use of non-nuclear EMPs to "fry" security cameras in banks among a variety of other systems.[31] The document provides numerous further resources to facilitate attacks against the financial services sector, in one instance recommending that readers watch a YouTube video titled, "How to rob a bank (And get away with it)," further inciting them to violence by calling them to "apply the knowledge and tactics discussed therein."[32] *RK* also shared instructions along with a discussion thread titled "Easy to make sticky thermite satchels for disabling vehicles" which mentions the use of thermite against armored vehicles. While the financial sector was not directly called out in this thread, the use of armored vehicles is a critically important part of the sector's supply chain to move currency between banks, ATMs and other financial institutions. Understanding

[31] *RK,* page 48.
[32] *RK,* page 88.

tactics discussed by DVEs for targeting armored vehicles is important for the financial sector in order to implement appropriate countermeasures.

Financial Services Sector Assessment: The tactics provided in *TKV* describing attacks and tactics against the financial sector are unsophisticated, incomplete, and impractical. Threat actor capability and sophistication would have to be very advanced to successfully conduct an attack against the financial services sector.

Conclusion: Summary of Risk to Critical Sectors

Risk to critical sectors is informed by the threat landscape, the potential consequences of successful attacks, and the probability of successful attacks. The extremist documents discussed here make only a minor contribution to the threat landscape overall for critical sectors because the information that they compile is neither innovative nor sophisticated. The theoretical capabilities of threat actors could be enhanced by this information despite consistent misconceptions regarding mechanisms and capabilities of law enforcement response, physical protections systems, and other factors. Nevertheless, these publications provide additional sources of radicalizing material and tactical guidance to support violent action.

Public safety personnel, stakeholders, and members of critical lifeline sectors can reduce risk by implementing thoughtful protective measures, processes, and other mitigations to reduce the consequences of potential threat actor activity. The probability of cascading failure of the electric grid due to an attack, especially if limited by the tactics and information described in these documents, remains very low due to the continuous work by the sector to improve the reliability, resilience, and security of the grid. However, concrete risks such as localized power outages and material loss can have real impacts to the efficiency and functionality of these sectors and critical services, increasing costs of service delivery. The cross-sector ISACs recommend that members and stakeholders continue implementing mitigations to reduce risk to their respective sectors. Additional information on existing resources related to risk mitigation options is provided in **Appendix A**.

Appendix A: Mitigations

According to the National Council of ISACs (NCI): *Information Sharing and Analysis Centers (ISACs) help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency*.

Consider getting involved with the critical sector ISACs contributing to this report:

Electric Sector:

- Electric grid AOOs, U.S. and Canadian government agencies, state, local, tribal, and territorial (SLTT) government agencies, national laboratories, cross-sector ISACs, and trade organizations are encouraged to join the E-ISAC Portal.
- The E-ISAC Physical Security Resource Guide provides a menu of resources related to physical security risk mitigation options.
- Review additional analysis on threatening discourse provided each month in the E-ISAC Monthly Online Threat Report.
- Reach out to 24/7 Watch Operations at operations@eisac.com or **202-790-6000** (24/7 hotline).

Water and Wastewater Sector:

Incidents can be reported to WaterISAC via any of the means identified below. WaterISAC recognizes the importance of confidentiality in reporting. Information identifying the reporting organization or individual is not disclosed to outside organizations without consent.

- **Online form** (accessible both on WaterISAC's secure portal and public website): www.waterisac.org/report-incident.
- **24-hour phone**: **866-H2O-ISAC (866-426-4722)**
- **Analyst email address**: analyst@waterisac.org
- **Physical and mailing address**: 1620 I Street, NW, Suite 500, Washington, DC 20006
- For more mitigation resources and other threat reports, please visit WaterISAC's resource center: https://www.waterisac.org/resources
- For more information on becoming a WaterISAC member, please visit this webpage: https://www.waterisac.org/membership

Healthcare Sector:

- Join the secure, vetted Portal, HTIP. Members include healthcare sector owners and operators tasked with protecting protected health information (PHI).
- See the Health-ISAC Physical Security Resources (available on the Health-ISAC Portal here) for more information on mitigations.
- Reach out to the Threat Operations Center at toc@h-isac.org.

Downstream Natural Gas Sector:

- For more information on the DNG-ISAC visit their webpage: https://www.dngisac.com/
- Join the secure, vetted Portal by reaching out via email: analyst@dngisac.com

Financial Services Sector:

FS-ISAC is the member-driven, not-for-profit organization that advances cybersecurity and resilience in the global financial system, protecting the financial institutions and the people they serve. Founded in 1999, the organization's real-time information-sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defenses. Member financial firms represent $100 trillion in assets in 75 countries.

- For more information about membership, please contact admin@fsisac.com. Members include:
  - Banks & Credit Unions
  - Core Back Office Suppliers
  - Critical Utilities
  - Exchanges
  - Fintechs
  - Insurance Firms
  - Investment & Securities Firms
  - MSSP
  - Payments
  - Trade Associations
- See our recent report Navigating Cyber 2024 for the latest threats, trends, and predictions for cyber and resilience for the financial sector this year.
- Operational concerns and intelligence can be submitted via sharingops@fsisac.com or **1 (877) 612-2622, prompt 2**.

Surface Transportation, Public Transportation, and Over the Road Bus and Surface Transportation Sectors:

- Join the Surface Transportation, Public Transportation, and Over the Road Bus ISAC Portal at https://surfacetransportationisac.org/membership/. Members include operators of trucking fleets, railroads, shipping and logistics infrastructure, manufacturing facilities, federal, state, and local government entities, foreign government agencies, and cross-sector ISACs.
- Reach out to the E-ISAC's 24/7 alert hotline at 866-784-7221.
- Any email inquiries should be sent to st-isac@surfacetransportationisac.org.

More information on other NCI member ISACs is available in the July 2020 NCI update providing general information on ISACs and the NCI.