Recommendations for Mitigating Risks to Electrical Substations in the United States:

Conducting Risk Assessments and Suggestions for Cost-Effective Solutions

Approved by: *Dr. Cheryl Banachowski-Fuller* Date: November 02, 2022

Recommendations for Mitigating Risks to Electrical Substations in the United States: Conducting Risk Assessments and Suggestions for Cost-Effective Solutions

A Seminar Research Paper Presented to the Graduate Faculty of

University of Wisconsin- Platteville

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Criminal Justice

Jason P. Wolf

November 2022

Acknowledgments

First and foremost, I would like to thank my wife, Anna, for all her support over the years. She has always been instrumental to my academic achievement throughout the pursuit of my undergraduate and graduate degrees. I also have to thank my family and friends for their support over the many years it has taken to reach this point in my academic career. Special thanks to the current and former Wisconsin Army and Air National Guard members that I have worked with on Antiterrorism and Force Protection matters over the years, especially Col. Shawn Gaffney, who provided insights into the unique characteristics of the Electrical Power Grid of the United States. Finally, thank you, Dr. Banachowski-Fuller and all of the professors and staff involved with the UW Platteville MSCJ program.

Abstract

This research paper aims to develop an effective and easily understandable methodology for conducting a risk assessment for electrical substations. Qualitative analysis was conducted using examples of existing secondary research, specifically, the collection of risk assessment methods, modes, and strategies currently being utilized across the critical infrastructure sector. Existing methods of assessing threat, vulnerability, and risk to critical infrastructure currently available, were explored to determine the best practices for developing a customized risk mitigation plan that can be tailored and applied to electrical substations based on current threats. Critical analysis was used to determine best practices that can be learned from case studies and applied when recommending new strategies moving forward in the development of a customized risk mitigation plan. Recommendations for a hypothetical electrical substation include a list of current threat scenarios and the risks associated with these threats based on common physical security measures used throughout the industry. Additional recommendations include building partnerships with local law enforcement and civilian stakeholders in the communities that these electrical substations provide service to.

Keywords: critical, infrastructure, threat, vulnerability, risk, assessment

TABLE OF CONTENTS

Introduction

With the recent mandate that 100 percent of new vehicles sold in California must be electric vehicles by 2035, the need for reliable and robust electrical power will be more critical than ever (California Air Resource Board, 2022). The current availability of consistent electricity across the United States varies based on what time of year it is and which region of the country is being evaluated (e.g., in the Southwest region during the summer, there are often issues meeting the electricity demands that the customers must deal with during the hottest days of summer). As is often the case, there will likely be additional states that follow California's lead and institute their own mandates for electric vehicles. This will cause additional demands for an electrical power grid that will need to be more robust than it currently is.

According to research by Phillips, "The United States has over 6,500 power plants supplying electricity across nearly 700,000 miles of transmission lines to approximately 150 million customers for an annual revenue of around $400 billion in electricity sales. It is the heart of the economy, powering industry processes and lighting, heating, and cooling homes and office buildings. It also is integral to health and safety, and access to affordable electricity is important to quality of life" (2019). The size and scope of the electrical power grid is immense and, as such, warrants as much protection and consideration as all other components that make up the critical infrastructure of the United States.

Statement of the Problem

Electrical power substations are critical as they are a single point of failure to electrical service in the area they service. The challenge lies with balancing the cost of securing these sites, with additional security patrols, compared to the perceived risk of a human-caused attack, as well as the effect on the community if electrical service is interrupted. Because these substations are

not provided adequate security, it falls on local law enforcement to respond to an issue or incident. Two recent incidents at electrical substations highlight the reality of these types of threats. The first was the theft and damage of $37,000 worth of equipment (Vogt, 2022). The second incident was vandalism which caused thousands of customers to lose power, and the estimated cost of the repairs was over $800,000 (Ball, 2022).

There are governing boards that set policies on how electrical power plants are secured; the Nuclear Regulatory Commission has specific requirements for the physical protection of nuclear power plants. Specifically, the use of Threat Assessments, Physical Protection Areas, Intrusion Detection, Intrusion Alarm Assessment, Armed Response to an intrusion, and Regulatory Initiatives that continue to evaluate requirements (2020).

The United States Air Force has long focused on the concept of Integrated Defense to protect its critical resources. According to the Air Force Policy Directive 31-1, “Integrated defense is the incorporation of multidisciplinary active and passive, offensive and defensive capabilities, employed to mitigate potential risks and defeat adversary threats to Air Force operations within the base boundary and the base security zone. These air and land threats include, but are not limited to, terrorists, insiders, foreign intelligence entities, criminals, and enemy forces. It is critical to incorporate integrated defense efforts with other Air Force, joint and combined capabilities to achieve synergistic effects using an all-hazards approach” (2018).

The concept and practices of integrated defense cannot be put into practice without understanding the need to develop a risk management process. The United States Air Force has taken the additional step of establishing a doctrine that addresses the Risk Management Process. The Air Force Doctrine Publication 3-10 defines Risk Management (RM) as “the process of identifying critical assets; understanding the threat; understanding Air Force vulnerabilities to the

threat; determining risk to personnel, assets, and information; and assuming risk or applying countermeasures to correct or mitigate the risk" (2019).

Adapting this doctrine to critical infrastructure is as follows- identifying how critical each component of the electrical power grid is compared to the other components; understanding the current threat to the specific component of the electrical power grid; understanding how vulnerable the component is to the threat. Once the Criticality Assessment, Threat Assessment, and Vulnerability Assessment are complete, the Risk Assessment can be determined. Based on the risk, the leadership of the utility company can make an informed decision on whether it is acceptable to assume the risk or develop a course of action to correct or reduce these risks. There are many examples of possible threats, and as such, it is an assessment that must continue to be updated. As the threat changes, the vulnerabilities can also change. For example, suppose the threat is vandalism or theft. In that case, the vulnerability assessment determines how easily a criminal can access the components of the electrical substation (e.g., there should be at least a fence and lighting around the area). However, if the threat is a natural disaster (e.g., flooding), the vulnerability assessment is concerned with whether or not the site is in a floodplain or lacks proper drainage for an excessive amount of water. The criticality assessment will remain relatively constant, unless there are significant changes to the number of customers that rely on the specific electrical substation. An example of this would be if a large manufacturing company moves to an area previously populated by a limited number of customers.

While it is true that utility companies do not have the personnel and resources, like the US Air Force, to dedicate to the protection of every electrical substation, the concepts can provide helpful insights on how utilities can prioritize their efforts and resources to more critical

electrical substations. However, there are still effective ways to reduce the vulnerability of the other substations that would be considered less of a priority.

Purpose of the Study

The purpose of this research is to assess risks to electrical power substations in the case of a power outage as a result of a human-caused attack on the power grid, and to make physical security recommendations based on best practices to mitigate these risks. Electrical power plants have significant security (Nuclear Regulatory Commission, 2020); however, the electrical power substations are primarily secured using fencing and gate secured with a padlock. While natural disasters can pose a significant threat to these electrical power substations, there are limited steps that can be taken to minimize the effects of some of the more likely natural disasters (e.g., ensuring that the area is not in a floodplain, or the equipment is elevated and has proper drainage). The desired outcome is that, at the very least, both natural and human-caused threats are identified, and the risk is either minimized or the utility companies decide to simply accept the risk due to the cost of providing additional security measures. Either way, the company, at the very least, can make an educated decision based on current threats and current technologies available.

Significance of the Study

This research paper will argue that there should be more focus on protecting electrical substations, which are single points of failure for the electrical power grid. The strategy that will be used to support the research presented is through successful vulnerability assessments already in use for other sectors of critical infrastructure in the United States. The successful elements of the vulnerability and risk assessments will then be combined to create a suggestion based on

evidence found for an ideal risk management program that incorporates best practices to be implemented across the electric power enterprise.

The field of Emergency Management focuses on developing Comprehensive Emergency Management Plans (CEMP), which plan for both natural and human-caused emergency situations (Haddow, et al., 2021). To that end, electric companies should adopt these same principles when protecting the various components of the electric grid. While little can be done to prevent a natural disaster, a CEMP will, at the very least, propose ways to mitigate the damage of a natural disaster. For instance, proper drainage and elevation of a substation can reduce the effects of flooding. When the threat of human-caused damage to a substation is considered, vandalism or theft are the most common scenarios. However, sabotage must also be considered and covers a myriad of scenarios or intentions.

There have been numerous incidents of electrical substations being shot at with rifles. A recent case involved a plot that was disrupted, and the conspirators were convicted (Department of Justice, 2022). While it would be difficult to prevent this type of attack, there are technologies that could be used as well as education of the members of the community around a substation that would aid law enforcement in their investigation after an incident.

The types of threats to electrical substations must be looked at through an “All Hazards” approach (ready.gov, 2021). This research is significant due to the steps for assessing criticality, threats, and vulnerabilities are similar for determining the risks of human-caused disruptions to electrical substations as well as determining the risks of disruptions due to natural disasters. The research provides a concept; however, each electrical substation is unique. Therefore, suggested guidelines are just that, a guide that utility companies could use to develop a course of action to correct or reduce these risks; it is not a blueprint that can be used in a “cookie-cutter” approach.

Developing risk management strategies that assist utility companies in determining the most cost-effective way to counter both current and future threats to their equipment requires constant attention. Criminals will adapt their methods based on changes in their environment. Through effective trend analysis and cooperation with local law enforcement, utility companies can make better-informed decisions. The concepts discussed in this research will not only assist with criminal threats, but also human-caused damage carried out for more nefarious purposes.

Therefore, this research will examine existing methods of determining the criticality of various electric grid components throughout the world, different crime prevention theories, and vulnerability and/or risk assessments currently in use for sectors of critical infrastructure. These methods will ultimately be used to provide recommendations for utility companies that will assist with the protection of these electrical substations. These recommendations will involve a variety of options which include high-tech as well as relatively low-cost solutions.

Literature Review

The literature review will consist of five sections. The first section is the summary of an article on multilevel planning for improving the resilience of critical infrastructure against power shortages. The second section addresses how critical infrastructure is related to a country's national security. The third section examines specific issues related to critical infrastructure in an urban area. The fourth will describe a unique initiative of the industry, and the fifth section addresses the education of the civilian population.

Multi-Level Planning for Improving Resilience of Critical Infrastructure against Power Shortages

The country of Sweden uses a system called STYREL, which is a Swedish acronym for "Steering of electricity to prioritized users during short-term electricity shortages" (Olausson, 2019). In a recent article, the STYREL system was examined in depth as a way to improve the

resilience of electrical infrastructure. The article divided the STYREL system into three objectives. First, the national government establishes the planning process. Second, the County Administrative Boards (CABs) are tasked with implementing the planning and providing feedback to both the national and county levels. Third, local municipalities identify consumers that are essential for the local population. Once these consumers are identified and ranked, lists are created and submitted to the respective CABs and complied and submitted up to the national government level (Große, 2021).

The STYREL system is not only used for the ranking of consumers of electricity. It provides insights for, "…both the Swedish crisis management system, which addresses the consequences of disturbances in societal functions, and the electrical power system, which is of vital importance for other critical infrastructure" (Große, 2021). The realization of the societal function disruptions is an essential function of an "All Hazard" approach to risk management planning (ready.gov, 2021).

Similar to areas of the United States, the Swedish government must contend with Load Shedding. California, for example, provides information to its citizens on why Load Shedding is necessary, explaining, "Load shedding is the temporary shutdown of electricity services, generally caused by statewide power shortages or problems on the Regional Electric Grid, insufficient power generation capacity, transmission constraints and/or risks of entire electric system failure" (Riverside California, 2016).

The Swedish government uses the information from the STYREL system to plan and implement Load Shedding. Power Grid Operators (PGOs), "…are legally obligated to independently perform this planning, which must permit each operator to disconnect at least 50% of the actual load" (Große, 2021). By planning for and confirming the feasibility of Load

Shedding, the PGOs are better prepared to deal with outages due to natural or human-caused events.

There are additional benefits to having this information and capabilities available to PGOs. One example is the reality that the electrical power infrastructure has to go through upgrades and other changes to the distribution needs of consumers. Due to this, "… changes in the grid's structure can cause the power supply to a particular power consumer to be realized via another power line than was assigned to this consumer during step three of STYREL" (Große, 2021).

The multiple uses of the STYREL system highlighted are a summary of the usefulness of this system. As is the case with many systems, the information is only as good as the information that is provided by the end users. If the information is incomplete or the information does not reflect the current environment, then the STYREL system is providing decision-makers with incomplete or inaccurate information. With this in mind, it is critical that individuals at every electrical power infrastructure level maintain current information and develop plans for future needs.

Critical Infrastructure's Importance to National Security

It would seem obvious that critical infrastructure would be "critical" to the national security of a country. Research focused on the county of Poland provides an in-depth analysis of the importance of critical infrastructure with respect to the national security of Poland. The components of critical infrastructure included "equipment, installations, facilities and services which are characterized, among others, by the following features: – long-term service life, – they serve as basic and specialized services, – they are public and serve the public, – they provide services for the industrial and consumer sectors, – they are owned by the State, corporations or

private individuals, – they are often international because of the network of connections and interdependencies (energy, telecommunications networks, etc.)" (Kosowski, 2019).

The research specifically highlighted and provided additional analysis of the liquid fuel supply and the electricity supply of the country. The specific concerns with these two sectors of the critical infrastructure included, "Long-term difficulties in this area always have serious economic consequences, lowering the security and comfort of life of citizens and disturbing their social life. For example, it is difficult to imagine the functioning of an agglomeration without electricity or drinking water supplies for more than a few hours" (Kosowski, 2019).

In the event of a significant loss of the liquid fuel or electricity supply, there could be dire consequences for the population and the security of the nation if the duration of the outages is more than a few days and/or involves a significant percentage of the country's population. This is especially true with regard to urban areas of a country.

Urban Critical Infrastructure: Emergency Management Considerations

In a study of a city in Nigeria, emergencies that had a high probability of occurring and causing a power outage were categorized. The three emergency situations were flooding, fire, and a vehicle crashing into components of electrical, as well as other infrastructure. The probability of a vehicle crash is based on the proximity of the components to roadways. The probability of flooding is based on the location of the component and "proximity to the flood channel or that the floodwater can cause a displacement in the location of the infrastructure" (Baloye and Palamuleni, 2017). The categories of very high, high, medium, and low probability of occurrence were used.

The study next looked at the frequency of these emergency situations happening to a component of the infrastructure. Frequency determination was based on historical data of flooding, fire, and vehicle crashes in the area being studied. The categories of very high, high, medium, and low frequency of occurrence were used.

The coverage that could be affected was classified as no coverage, partial coverage, or total coverage. These categories are defined as "no coverage, implying that no area occupied by the critical infrastructure is affected; total coverage, signifying that the event, say flood, can affect the total area occupied by the critical infrastructure, for instance, the spatial relationship between flood and bridges; and partial coverage, which signifies that the event can occupy some part of the geographical area covered by the critical infrastructure" (Baloye and Palamuleni, 2017).

The final category is the extent of damage that could affect the infrastructure components. Again, the categories were very high, high, medium, and low. The study found, "In terms of the extent of damage to critical infrastructure, flood shows the least possible damage followed by automobile crash and then fire. Also, the extent of damage on critical infrastructure components suggest that fire outbreaks tend to affect more the critical infrastructure components compared to flood and automobile crash. Furthermore, it can be noted that damage on electricity distribution components is common under the three emergency events…" (Baloye and Palamuleni, 2017).

The following charts are simplified versions of the charts in this study and provide a useful guide to assist decision-makers in prioritizing not only which components to restore after a power outage, but also assist in prioritizing preventative maintenance (Baloye and Palamuleni, 2017). For simplicity, the scenarios of Flooding and a Vehicle Crash will be used as examples as

these examples were used in the article. However, the vehicle crash could be easily substituted with vandalism or theft at the respective location.

Location Priority	Probability of Flooding	Frequency of Flooding	Coverage	Extent of Damage
1	Low	Low	Partial	Low
2	High	High	Total	High
3	Medium	Low	Partial	High
4	Low	Low	Partial	Low
5	Low	Low	Partial	Medium

In this chart, the highest priority location has a low probability and frequency of being affected by flooding. Additionally, the coverage and damage expected are relatively low. However, the second highest priority location is very likely to be affected by flooding, and the damage and coverage area would be significant. Based on this information, more resources would be needed to reduce the effects of flooding at this location. This could be additional drainage ditches or building up the location with sandbags before significant rainfall.

The next chart looks at the effects of a vehicle crash on the same hypothetical locations. In this scenario, the highest priority location is, in fact, located in an area that is prone to vehicle crashes. Not only that, but the amount of damage would also be high and large areas of coverage would be affected. In this scenario, resources would be needed to mitigate the damage of a vehicle crash near this location. This could include installing bollards around the perimeter of the site.

Location Priority	Probability of Vehicle Crash	Frequency of Vehicle Crash	Coverage	Extent of Damage
1	High	High	Total	High
2	Medium	Low	Partial	High
3	Medium	Low	Partial	Low
4	Low	Low	Partial	Low
5	Low	Low	Partial	Medium

Again, these are simplified charts due to the charts provided in the study used acronyms for a multitude of locations. The examples provided by these simplified charts would assist decision-makers with prioritizing not only which components to restore after a power outage but also assist in prioritizing preventative maintenance as well as justification for additional protective measures to mitigate risks. For example, typically, the highest priority electrical infrastructure would be near a highly populated area. However, there could be a scenario where a rural area has an industry that is of significant importance. For example, if there was a chemical plant in a rural area, it would be critical for the safety of the plant that electrical power was not interrupted.

Deep Learning for Improving Critical Infrastructure Resilience

In a recent case study, the concept of Deep Learning was studied as a viable option to assist in the protection of critical infrastructure. Deep Learning is, "emerging as an effective way to create and train highly accurate machine vision systems, requiring only labeled images as input" (Dick et al., 2019). In simpler terms, Deep Learning is a type of Artificial Intelligence. However, the difference with Deep Learning is that "both the decision function and the data representation are simultaneously learned and optimized from the training data. The word deep refers to the high number of layers… typically used in such a network" (Dick et al., 2019).

The end goal of using Deep Learning appears to be a more efficient way to identify threats or situations where the electricity supply is in question. An example of this would be the use of Deep Learning to identify areas or specific components of the Electrical Grid that require preventative maintenance to reduce the likelihood of power outages in the immediate future. This objective prioritization of how and when preventative maintenance should be done, as well as

which specific location or component must be completed before other locations or components, help decision-makers effectively deploy their assets.

The benefit of Deep Learning is that it provides increased capabilities for monitoring and determining changes in the environment compared to a trained individual. According to Dick et al., “For an individual to rapidly identify these objects of interest, they may be exposed to practice feeds to hone their perceptive ability, and the officer’s accuracy improves with time and experience” (2019). However, this would require the individual to maintain a very high level of concentration for extended periods of time. The reality is that an individual has to take breaks to prevent fatigue.

Research has begun on the use of Unmanned Aerial Vehicles (UAV), more commonly known as drones, as part of a Deep Learning system to monitor and assess sections of the electrical infrastructure. “Machine vision analysis of UAV captured aerial images for the detection of power transmission lines has been investigated by a research team in Bangalore, India, and they achieved upwards of 99% accuracy” (Dick et al., 2019). This example uses limited datasets; however, it certainly shows promise for future research.

These types of technological advancements and experiments demonstrate the importance of the electrical infrastructure of a country. And these advancements come at a time when the risks to a country’s critical infrastructure are more profound than ever. “Power outages and the required repairs to the power grid in the United States have been estimated by America’s Electrical Cooperatives to be at least $177 billion in this coming decade because of the aging infrastructure” (Dick et al., 2019).

The importance of consistent and reliable electricity for a country cannot be overstated. Nearly everything a population needs to survive and succeed in their respective lives uses electricity. “Notably, transportation networks are threatened by energy disruptions, the finance and banking sectors rely on electricity for operations, and telecommunication systems rely on continuous power. Food- and water-related resources are reliant on the energy infrastructure for their supply chains” (Dick et al., 2019). One way to compare the electrical infrastructure to other components of infrastructure would be to look at the infrastructure of roads and highways. If a road is closed or shut down, other roads can likely be used to still get to a destination. If electrical power is shut down, other than using backup generators, which typically only provide minimal power to sustain critical functions until the electrical power is restored, there really are no viable options to continue operating.

Comparative Analysis of Education of the Populace for Critical Infrastructure Collapse

An article focused on the United Kingdom, the United States, Germany, Japan, and New Zealand compared how well the civilian population is informed on the issues that could significantly affect the critical infrastructure of their respective countries. The terms used throughout the article are CI (Critical Infrastructure) and CIP (Critical Infrastructure Protection). The article had three goals, “The first is to understand the complexity of the contexts within which systems and policies for CIP have been developed…Secondly, the project aims to identify gaps between governments’ perceptions of how the populations would respond in case of a national crisis… Thirdly, the project aims to understand population response which informs emergency planning” (Kitagawa et al., 2017).

The United Kingdom and the United States government view CIP as classified information and therefore, the civilian population is not well informed on the risks and threats to CI in their respective country. It appears these countries have decided that because there are government agencies that are charged with the protection of CI, there is less need to educate the civilian population and instead focus on protecting the "classified" information. This is shortsighted, as much of the information is available online if someone was so inclined to search for it (Kitagawa et al., 2017).

Germany is a bit different from the other countries that were included in this article in that it, "…does suffer from severe weather events and flooding, and terrorism is regarded as a risk. It is, however, relatively open about its approach to CIP" (Kitagawa et al., 2017). With that said, the German government does not appear to educate the civilian population on the severity of the threats to CI. In fact, "The general population in Germany remains comparatively under-educated and under-prepared for disaster, with very low levels of awareness about the interconnectedness of the CI and the implications of both past and future disasters for their lives" (Kitagawa et al., 2017).

Japan, due to it being an island, is prone to severe weather and other natural disasters and therefore takes a pragmatic approach to educating and empowering the civilian populace. There have been recent disasters in Japan that highlight the need for all citizens to prepare for these realities. In fact, the government of Japan provides tools, "… to advocate the population to prepare and protect themselves in case of a crisis, rather than waiting for the state's instruction and support" (Kitagawa et al., 2017).

New Zealand also is prone to severe weather and other natural disasters and, "…has long been aware of the need to take a structured and coordinated approach to protecting the national

infrastructure and strengthening resilience at all levels (social, political, economic), and the approach taken is considered very innovative" (Kitagawa et al., 2017). The fact that both island countries, Japan, and New Zealand, take these threats to CIP seriously enough to involve the civilian population is noteworthy. Especially when considering that the United Kingdom, also made up of many islands, has not adopted a similar approach to CIP.

The studies and articles discussed in this literature review demonstrate not only the reasons that the electrical power grid is one of the most critical components of a country's critical infrastructure, but also provide insights on steps that can be taken to improve the reliability of electricity being provided. The first steps of conducting risk assessments involve determining the criticality and priority of the assets to establish the need for protection.

In the following section, the theoretical framework will be discussed that relates to ways to prevent, or at least, minimize human-caused damage to electrical substations. The theories discussed are Crime Prevention Through Environmental Design, Defensible Space Theory, and Situational Crime Prevention Theory.

Theoretical Framework

The theories of Crime Prevention Through Environmental Design, Defensible Space, and Situational Crime Prevention have long been used to reduce criminal behavior in urban areas and, in one case study referenced in this section, to address poaching. Using these theories to enhance the design and physical security of electrical power substations will assist decision-makers in prioritizing future funding and efforts. These theories highlight ways to not only prevent human-caused damage to electrical power substations but also provide the civilian

population with proactive steps that can be taken to better monitor these components of critical infrastructure.

Crime Prevention Through Environmental Design Theory

The concept of designing an environment that aids in the prevention of crime has been an accepted practice for some time. According to Mihinjac and Saville, "For example, many city governments now employ Safe City plans with safety strategies and [livability] indices in which they [recognize] the synergy between urban form, crime, and social conditions" (2019). The concept of crime prevention through environmental design (CPTED) has been updated over the years and is differentiated by the terms First-Generation and Second-Generation CPTED. First-Generation focused on reducing opportunities to commit crimes through physical or architectural designs. Second-Generation added strategies that addressed conditions and social relations in neighborhoods (Mihinjac and Saville, 2019). There is also a Third-Generation of CPTED; however, it proposes ways for residents to fulfill higher needs according to Maslow's Theory of needs (Mihinjac and Saville, 2019) and as such, will not be dealt with in depth in this section.

Another notable difference between First and Second-Generation CPTED is that "… First-Generation modifications change the environment within a short timeframe, whereas Second-Generation social strategies aim to build a sense of community and social cohesion over a longer period of time" (Mihinjac and Saville, 2019). This can be applied to the protection of electrical power substations when considering how to involve and educate the surrounding communities on the need for their assistance when it comes to preventing and reporting crimes committed that affect these electrical substations.

The physical security of an electrical substation often involves perimeter and area lighting to assist with deterring or at least identifying trespassers on the property. This design is often proposed in the generations of CPTED, "Improved lighting to enhance natural surveillance in dark areas might result in aesthetic improvements to dark areas like parks or walkways. However, in First-Generation CPTED, the intention of improved lighting is to increase guardianship through the improved natural surveillance of a high-risk area" (Mihinjac and Saville, 2019).

In another research article, the importance of proper lighting is discussed in more detail, and Information and Communication Technology (ICT)-based surveillance. The researchers proposed, "an ICT-based framework that connects place (potential crime scenes) and space (spatial characteristics and perception) to dynamically improve the spatial characteristics of potential crime scenes towards deterring and discouraging crime by controlling lighting parameters" (Vogiatzaki et al., 2020). This framework assists with the creation of a "smart city".

The different approaches to a smart city include, "(a) the technology-oriented approach, i.e., platforms, applications and model; (b) the people-oriented approach, i.e., stakeholders, citizens, knowledge, services" (Vogiatzaki et al., 2020). The combination of these approaches would be the ideal way to protect electrical substations. Technologies (e.g., lighting, intrusion detection sensors, CCTV cameras, etc.) and educating the civilian population and other stakeholders in the community.

The most prevalent technology used for crime prevention is lighting. It has been found that, "lighting can affect crime indirectly through two mechanisms. Firstly, by enabling people to recognize the intentions of others, see well all around and allow better surveillance. Secondly, by enhancing community confidence and increasing the degree of informal social control"

(Vogiatzaki et al., 2020). As such, at a minimum, electrical substations should have lighting that is employed in a way that deters criminals or, at the very least, assists with identifying them.

Finally, Vogiatzaki et al., found that the following three observations are common throughout previous research:

> Crime can be prevented by (a) a clear demarcation between public and private space, (b) eyes on the street, (c) continuous use of streets;
>
> The possibility of informal control by residents can create defensible space coupled with feelings of territoriality;
>
> Previous crimes can identify areas that are crime-prone, since offenders make rational choices and operate in areas they know (2020).

Using these concepts and findings, efforts should be taken to adopt these principles to improve the design and educate stakeholders. To further address the improvement of design, Defensible Space Theory provides additional recommendations.

Defensible Space Theory

There are similarities between CPTED and Defensible Space Theory. Defensible Space Theory often involves the use of passive ways to deter crime; it "… focuses on design standards that can improve architecture, land use, security and lighting, and places significant emphasis on territoriality and the need for residents to gain a sense of ownership; which is needed in order for the design to be effective" (Piroozfar et al., 2019). Active ways to deter crime would include security patrols, active monitoring of CCTVs, etc. The Defensible Space Theory was inspired by the demolition of a housing complex in St. Louis, Missouri in 1972 (Piroozfar et al., 2019).

Another aspect of the Defensible Space Theory is the posting of signs. The reason is that "The idea of signage is to provide information and encourage users to utilize the space and to use it as intended. It also helps differentiate between public and private spaces" (Piroozfar et al.,

2019). An added benefit of posting signage is that it aids in the prosecution of trespassers if "No Trespassing" or "Private Property" signs are posted. Another way to define Defensible Space Theory is, according to research by Muhyi et al., "a model for residential environments which inhibits crime by creating the physical expression of a social fabric that defends itself" (Newman, 1972, as cited by Muhyi et al., 2019).

Recently, a study of two housing areas in Indonesia compared the effectiveness of defensible space. One discovery was, "…defensible space can only work well if the social conditions of society are in an optimal state because even if an environment has been architecturally designed, it is still unsafe if the social climate is unwell. Therefore, it can be concluded that the behavior formed from defensible space is influenced by physical and social conditions" (Muhyi et al., 2019). The two housing areas were the Babakan Residence (BR) and Pulo Geulis (PG).

The BR housing area has "…high and closed fences and CCTV in some houses, it shows that the houses are very restricted from outsiders. However, the overall boundaries of this residential area itself are not so clearly created as there is no boundary separating the area within the residence with the outer area surrounding the residence" (Muhyi et al., 2019). In this area, technology is used however, it is not clear where property lines end and begin. The actual residence is the only reference point of property delineation. It should also be noted that the BR housing area has private security that monitors the area which leads to the expectation that the residents are of higher class compared to the residents of the PG housing area.

In the PG housing area, there are natural boundaries that "… restrict the area of the kampung to the outside area with the presence of the river as a very clear delineation, while the boundaries on each house are not so clear" (Muhyi et al., 2019). However, the lack of boundaries

for each house is not as much of an issue because the natural boundaries have the effect of keeping non-residents out of the area.

There is also a significant difference between the housing areas with how surveillance is conducted by the residents. In PG, “natural surveillance is created through open doors and windows and directly facing the road ahead, semi-private and public fusion zones, and unlimited visual access” (Muhyi et al., 2019). The residents of PG rely on human interactions and experiences to determine who belongs in the area and who is out of place. The BR residents over-rely on fences; however, “High and closed fences cause blockage to house’s windows so that residents cannot monitor outside space from inside their houses” (Muhyi et al., 2019). In this comparison, while fences may give people the feeling of security and safety, if the fences are not located in the proper area or not properly maintained- they can ironically become a barrier the criminal can use to their advantage.

The PG residents have a more effective deterrent effect on crime that is also more cost-effective. This obviously took time to establish, however when natural surveillance is prevalent, “the crime rate can be reduced even if the occupant is in or away from home and does not require the use of security devices or the role of security apparatus” (Muhyi et al., 2019). The additional benefit of this scenario is that the residents are preventing situations that would encourage criminals.

Situational Crime Prevention Theory

A simplified definition of Situational Crime Prevention Theory is, “Situational crime prevention focuses on the settings where crime occurs, rather than on those committing specific

criminal acts" (College of Policing, 2022). Essentially the focus is on identifying environmental conditions that do not discourage crime.

According to the Center for Problem-Oriented Policing, the following five ways can be used to address situational crime:

> Increasing the effort the offender must make to carry out the crime.
>
> Increasing the risks the offender must face in completing the crime.
>
> Reducing the rewards or benefits the offender expects to obtain from the crime.
>
> Removing excuses that offenders may use to "rationalize" or justify their actions.
>
> Reducing or avoiding provocations that may tempt or incite offenders into criminal acts (2022).

The first three would involve efforts and techniques that could be considered objective in nature. Installing a fence with barbwire would increase the effort, installing CCTV would increase the risk of being identified, and working with pawn shops or recycling locations to ensure that they confirm items they purchase are not stolen would make it difficult to sell stolen items.

Research was conducted on how Situational Crime Prevention Theory could be applied to the crime of poaching in Africa. What was discovered is that the crime of poaching typically occurs in an area where there is little chance of the crime being witnessed. Also, due to the dire economic conditions of the countries where poaching is prevalent, there is a higher likelihood that people will accept bribes to look the other way. With these issues in mind, the focus on enforcement of anti-poaching laws would be more effective when dedicating resources to monitoring the locations where poached animals are "…collected for transport and where inspections can be carried out" (Huisman and van Erp, 2013).

The theories and ideas discussed in this section are useful when assessing vulnerabilities to critical infrastructure components. In the following section, a program evaluation will focus on current examples of vulnerability and/or risk assessments in critical infrastructure.

Program Evaluation: Current Examples of Vulnerability and/or Risk Assessments in Critical Infrastructure

The previous sections have addressed techniques to assess the criticality of infrastructure components as well as ways to assess the threats to these components. In addition, various theories have been discussed that provide insights into some of the reasons that criminals commit crimes and ways to both design and maintain a site in an effort to deter criminal activity.

The Vulnerability Assessment (VA) is a product that should be continuously reviewed based on trend analysis as well as changes to the environment or area where these electrical substations are located. In addition, as improvements are made to these locations, the vulnerability to certain types of threats could be reduced. In these scenarios, the previous VA should be reviewed to ensure that it is still relevant.

Lao Power Sector Vulnerability Assessment and Resilience Action Plan

In a recent in-depth report on the country of the Lao People's Democratic Republic, Stout et al., defined the term VA as "A comprehensive assessment of the Lao PDR power sector's vulnerability to climate and [non-climate] natural hazards and to human and technological hazards" (2020). This type of "all hazard" approach to conducting assessments is a proven technique when the goal is producing a product that is objective in its findings (ready.gov, 2021). See appendix for an illustration of the VA process.

Stout et al., used an eight-step process for not only the VA but also for developing an action plan to increase the resilience of the power sector. The steps are:

1. Collect information about hazards and hazard impacts
2. Assess vulnerabilities
3. Conduct planning to increase resilience in the power sector
4. Develop resilience actions
5. Implement resilience actions
6. Monitor and evaluate the effectiveness of resilience actions
7. Report on the impacts of hazards and the effectiveness of resilience actions
8. Adjust plans and measures for increasing resilience based on the results of monitoring and evaluation (2020).

For any assessment to be useful, the information that is inputted is key to the success and usefulness. The six types of information that are key when conducting a comprehensive VA are:

1. Scientific assessment of the existing information on the current and past impacts of climate
2. Scientific assessment of forecasts of future changes in climate
3. Projected impacts of climate change
4. Scientific assessment of other natural-hazard (such as earthquakes) information on the current and past impacts of natural-hazard events
5. Assessment of other hazard data (such as the number of accidents causing outages) and the associated impacts
6. Assessment of the changing conditions under which human-caused hazards exist within the power sector (Stout et al., 2020).

Stout et al., note that decision-makers need to examine all hazards when addressing vulnerabilities and these identified vulnerabilities require realistic steps that can be taken to mitigate the effects these hazards would have on critical infrastructure components (2020). See appendix for an example of a table that lists potential hazard types and vulnerabilities.

Once the vulnerabilities are established for the critical infrastructure components based on an all-hazards approach, a risk assessment can be completed. Stout et al., emphasized that, “Changes in climate and [non-climate] hazards, and changes in the physical, social, economic, or natural environment affect the results of a VA and the priorities that emerge” (2020).

The report on the country of the Lao People's Democratic Republic, takes the next step in the risk mitigation efforts and establishes a plan to increase the resiliency of the Electrical Power Infrastructure that, "outlines a step-by-step process for implementing resilience actions. The plan should identify the implementing lead, describe costs and financing of solutions, and clearly define all intermediate steps in resilience solution implementation" (Stout et al., 2020).

What is key for decision-makers is that the process for conducting a VA is consistent across the board. This approach to conducting VA is an excellent example, however, it is not the only way to conduct a VA.

A Model-based Systems Engineering Approach to Critical Infrastructure Vulnerability Assessment and Decision Analysis

In a study conducted by Huff et al., standards for the critical infrastructure industry and previous significant incidents were researched. One significant incident was a coordinated attack that "…occurred in April 2013 at the Pacific Gas and Electric Corporation Metcalf substation where gunmen fired bullets at the substation and damaged 17 transformers and 6 circuit breakers which resulted in an estimated $15.4 million in damage" (2018). Based on the specifics of this incident, recommendations are made on enhancements that decision-makers can take to better mitigate the effects of similar human-caused incidents. See appendix for a detailed description of this incident.

Physical Security Recommendations

With regard to the type of physical barriers that would reduce the vulnerability of damage sustained by bullets fired at transformers, walls would be more effective than chain-link fencing, which was the case at the Metcalf substation. Huff et al., found that, "Solid walls are generally more difficult to breach and also prevent direct line-of-sight access to equipment inside the

substation. Solid walls may prevent external vandalism, such as gunshot damage, depending on the height of the wall, surrounding terrain, and elevation of equipment inside the substation" (2018).

Huff et al., also recommend the use of CCTV that can be monitored remotely and have the capability to automatically detect movement or alarms being activated. An additional benefit would be the video feed being recorded for the investigation of such an incident- which was the case at the Metcalf substation.

The lighting in and around a substation should also be considered an important element of the physical security of a substation. "The entire interior of the substation may be provided with dusk-to-dawn lighting to provide a minimum light level of 21.52 Lux (2 footcandles). Placement of lighting posts should be such as not to assist an intruder who may climb the posts to enter the substation. All wiring to the lighting posts should be in conduit or concealed to minimize tampering by an intruder" (Huff et al., 2018). One consideration regarding lighting is the local laws where the substation is located as there might be limits to how bright these lights can be.

The last physical security recommendation that was made was the use of security patrols at substations that are located in areas where there is a history of vandalism and theft. However, this can be cost-prohibitive if needed for an extended amount of time. If this is the case, it is recommended to form a good relationship with local law enforcement. In either case, planning and procedures for how alarms response should be prioritized as well as unique situations that would require additional security until the situation has been resolved. Huff et al., mention, "…during special or unusual occasions, such as labor disputes, the Olympics, or a presidential

visit, security procedures at critical substations may include identification checks by security patrols and limited access to the substation" (2018).

Determining Future Types of Incidents

The types of incidents that have a high probability of occurring need to be considered. As enhancements are made to a substation, the tactics used by nefarious actors will likely change. Huff et al., theorized that, "… a possible future attack could be jamming the wireless communication systems used for security resources in the substation" (2018). For the purpose of their research study, the scenario of a disgruntled employee disabling the wireless connection for surveillance CCTV was used for planning purposes. This type of "Insider Threat" scenario is certainly within the realm of possibility (Huff et al., 2018).

No matter the particulars of a specific substation and the environmental or human-caused threats that exist, awareness of these issues is a critical component to identifying and mitigating risk. "Awareness can be improved by (a) Providing tutorial information to employees. (b) Using posters on-site. (c) Circulating information on reported incidents. (d) Using a site security checklist. (e) Encouraging suggestions for improvement. (f) Marking tools with company identification. (g) Encouraging customers and property owners to report suspicious activity around facilities" (Huff et al., 2018).

Whether or not the attack on the Metcalf substation was an act of terrorism is still not clear- as to date, no suspects have been identified. For the purposes of a vulnerability assessment, whether it was an act of terrorism, or the act of a disgruntled employee does not matter. It is the tactic used, not the motivation for the attack, that is considered when decision-makers have to prioritize where enhancements will be made to these substations.

Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation

As mentioned previously, there was a recent case involving a plot that was disrupted, and the conspirators plead guilty to Domestic Terrorism (Department of Justice, 2022). This case had many similarities to the Metcalf substation incident. Any VA conducted would certainly need to consider the realistic threat of terrorism. In fact, many of the scenarios of human-caused incidents could in fact be an act of terrorism masquerading as an accident or vandalism.

Yao et al., proposed an innovative approach, "…to simulate strategies used to protect the CI against terrorist attacks, as well as the authorities' reactions to such attacks, a game-theory approach is selected as the basis for a vulnerability assessment…" (2020). In addition to the use of game theory, their approach also looked specifically at the country of Israel and how the terror attacks, on an actual substation in that country, can be addressed in such a way that is within the limits of budget constraints (Yao et al., 2020).

Yao et al., not only assess the vulnerability of specific components of CI in an area, but also the secondary and tertiary effects on other CI components that are interconnected and interdependent (2020). These considerations can be "broken down into two basic types: (1) direct losses on functionality of the components in the system, and (2) indirect effects arising from interactions between or among multiple components" (Yao et al., 2020).

For the discussion on the use of game theory for protecting CI, Yao et al., used scenarios where, "The protection process is modeled as a zero-sum game, which means that while the defenders try to minimize the potential [loss] after the attack, the attackers aim to maximize [lose] by allocating limited resources" (2020). In other words, decisions would be made by defenders to provide adequate protection that would deter all but the most determined attackers.

The attackers would make decisions on the amount of effort it would take to defeat the protection that the defenders have established. The limiting factors in this scenario would be the amount of protection that the defenders can put into place (based on budget constraints) and the number of resources and personnel that the attackers have at their disposal to perpetrate an attack.

The findings of the study conclude that, "The methodology proposed makes it possible to optimize the investment to critical infrastructure protections at lower levels, which can help to reduce expenditures on local infrastructure protection or on a single critical infrastructure for small projects" (Yao et al., 2020). Using the Metcalf substation attack as an example, the cost to repair the substation was over $15 million. Therefore, this amount can be used as a reference for substations that are similar in size and design when determining how much decision-makers could realistically spend to increase the physical security at a substation to prevent a similar attack.

In a previous study coauthored by one of the authors, and referenced in this study, there are 5 levels of protection recommended for substations in Israel that were likely targets of terrorist attacks. These suggested solutions were measured according to the Protection Effectiveness (PE). Here were the findings:

> For example, the protective solutions for the robustness strategy included: full protection of steel construction (PE=0.99), protection by concrete construction (PE=0.90), burial of critical components in the soil (PE=0.65), protection by partitioning concrete walls (PE=0.50), protective secured space (PE=0.35), and without protection (PE=0.01). For each level of PE a calculation of the risk expectancy analysis was carried out. The outcomes of the annual attack probabilities are found to be 0.253, 0.303, 0.358, 0.408, 0.487, and 0.606 respectively (Elkabetsa and Shohetb, 2015).

Put simply, full protection through steel construction provides the best PE (.99) whereas a site without any protection (which is not considered one of the five levels or protection) does not

have any PE (.01). The midpoint of the PE scale is the use of partitioning concrete walls (.50). See the appendix for an image of these types of walls actually in use at a substation. Again, these protective suggestions were for substations in Israel that would likely be attacked with high-grade explosives however, these measures offer insights into the options available.

One additional statement of the study is the awareness of how terrorists can utilize the internet and other media to conduct target selection. Quoting the al Qaeda training manual, "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy" (Yao et al., 2020). The image of the types of walls actually in use at a substation, provided in the appendix, demonstrates how this type of information can be gathered and decision-makers should be informed that substations they are responsible for likely have similar images on the internet.

A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid

The discussion would not be complete without briefly covering cyber threats that affect the electrical power supply. Typically, the greatest threat is to the electrical power production equipment, as it is connected to some type of network or at the very least, the use of technology to produce electricity safely and efficiently. Baggott and Santos found that, "Most of the previous risk-related studies on the electric power grid focus mainly on the recovery of the network from hurricanes and other natural disasters. In contrast, a disproportionately small number of studies explicitly investigate the vulnerability of the electric power grid to cyber-attack scenarios, and how they could be prevented or mitigated" (2020).

While the topic of cyber security threats to the entire electrical power grid would be too detailed to be covered in this research, looking specifically at possible cyber-attacks that could

affect a substation is a more realistic focus of this research. Three simple questions were identified by Baggott and Santos' (2020) research, "(i) What can happen? (i.e., What can go wrong?), (ii) How likely is it that that will happen? (iii) If it does happen, what are the consequences?" (Kaplan and Garrick, 1981). In the case of a substation, one technology that could have something "go wrong" would be the network connection for alarms and CCTV at a substation. The likelihood of this occurring is indeed possible, as the Metcalf substation attack showed that the attackers appeared to target the communications lines to the substation specifically. Cybercriminals could likely accomplish similar results to communication networks. Finally, the consequences could be severe if the loss of communication with a substation was not discovered quickly enough to dispatch a technician to reestablish the communication connection. In the interim, at the very least, a security patrol or local law enforcement would be dispatched to the substation to conduct a security check. There will be costs associated with having a security check conducted, as well as the cost of the technician to determine the cause of the loss of connection. The worst case would be a scenario like the Metcalf substation (Huff et al., 2018).

One threat scenario would be an insider threat, for example, a disgruntled employee that divulges network vulnerabilities or installs malicious software into the network or specific components. When determining ways to counter these threats, Baggott and Santos' research identified the following three risk management questions, "(1) What can be done and what options are available? (2) What are the trade-offs among costs, benefits, and risks? (3) What are the impacts of current decisions on future options?" (Haimes, 1991, as cited in Baggott and Santos 2020). When determining the threat of disgruntled employees, the options available would be, first and foremost, ensuring that the hiring process includes an extensive background check of prospective employees. In addition, periodic background and financial checks on

current employees can assist in determining if an employee is having personal or financial problems. There would be costs associated with conducting these types of checks; however, the benefits of identifying employees that are struggling and providing them with resources will increase their productivity and illustrate that the company cares about its employees. The impact of more productive employees would pay dividends in the future.

The threats to critical infrastructure are certainly vast. However, there are steps that can be taken that address these various threats. A vulnerability that is addressed to counter a criminal threat could also counter a terrorist threat. Improving the hiring practices of a company would not only help reduce the threat of a disgruntled employee installing malicious software but could also reduce workplace violence if the periodic background and financial checks reveal that an employee is at risk of having some sort of life crisis that could cause them to become violent. What is needed is an all-hazard approach to assessing risk and ensuring that these assessments are conducted frequently in an effort to take new trends, threats, or environmental changes into account.

Various United States government departments and agencies have utilized risk management tools and strategies. One such tool is the use of the CARVER acronym for determining how terrorists or other nefarious actors would view a specific target or location.

> **C**riticality - measure of public health and economic impacts of an attack
> **A**ccessibility – ability to physically access and egress from target
> **R**ecuperability – ability of system to recover from an attack
> **V**ulnerability – ease of accomplishing attack
> **E**ffect – amount of direct loss from an attack as measured by loss in production
> **R**ecognizability – ease of identifying target (Food and Drug Administration, 2018)

The United States Air Force has nine desired effects of Integrated Defense. They are "Anticipate, Deter, Detect, Assess, Warn, Defeat, Delay, Defend and Recover" (2018).

Anticipating threats can be achieved through crime trend analysis and past natural disasters. Deterring criminals and other bad actors is typically accomplished by placing barriers and signage that increase the risk of being caught committing a crime. Detection is dependent on either security patrols on scene or through the use of intrusion detection systems (IDS), commonly referred to as an alarm system. Assessment requires the immediate identification of who or what is causing the alarms. Warning other locations would be the desired response if responding personnel confirm that indeed there is a crime that is or has occurred. Defeating the criminals typically occurs when there are security patrols already on scene, however, this is unlikely in the case of electrical substations. Delaying a criminal act can be achieved by placing significant barriers, thus causing the criminal to take an extremely long time to commit the crime. Defending the site would again, require the use of security patrols and is unlikely to be the case at an electrical substation. Finally, recovery is a consideration that decision-makers have to make. Put simply, this has to do with how long it would take to restore electrical power after the event (either natural or human-caused).

Recommendations

This recommendation section will focus on some of the Desired Effects of Integrated Defense that the US Air Force has developed that pertain to the protection of Critical Infrastructure, the CARVER methodology for determining criticality and vulnerability, and finally, highlight some of the unique methods that are currently used in assessing vulnerabilities and risks to components of critical infrastructure that have been mentioned in previous sections.

Ideal Components for Risk Assessment Program Overview

There are certain components that are needed for the protection of electrical substations that utility companies should consider when deciding what steps need to be taken. The use of the

United States Air Force's nine desired effects of Integrated Defense of "Anticipate, Deter, Detect, Assess, Warn, Defeat, Delay, Defend and Recover" would provide a framework on which to build (2018). For the most part, these electrical substations will not have security patrols on site unless there is significant work being done at the site that would warrant the cost of providing security patrols. Because of this, Defeat and Defend will not be addressed in this recommendations section and instead, the focus will be on the other seven desired effects.

Anticipate

Being able to anticipate what the current threats are to an electrical substation is one of the first considerations when developing countermeasures that address these threats. For example, the threat of a criminal or nefarious actor using a rifle to attack the components of the substation can be countered by installing walls that offer adequate protection to stop bullets from penetrating vulnerable components. There is a tradeoff with installing walls, and that is the obstructed view of the area- this can be countered through the use of CCTV to enhance the ability to observe these "blind spots." Continued trend analysis and working relationships with local and federal law enforcement will also provide insights into emerging threats.

Deter

There are many physical security improvements that can deter all but the most committed criminals from attempting to access an electrical substation. Fencing and signage provides an obvious and legal boundary for the site as well as shows a criminal's intent if they ignore the signs and climb the fence to illegally gain access.

Detect

Detection is typically achieved by using alarms, commonly known as Intrusion Detection Systems (IDS) in the industry (USAF Police Alumni Association, 2021). There is an obvious

cost to install these types of IDS as well as the communications required for the alarm system to notify either a security company or law enforcement.

Assess

Assessment is achieved through either an Immediate Visual Assessment (IVA) using CCTV on-site or by dispatching either a security patrol or law enforcement (USAF Police Alumni Association, 2021). What is key to an effective assessment is determining the average response time of the security patrol or law enforcement.

Warn

The ability to warn other decision-makers in the critical infrastructure industry will assist during periods of civil unrest or when new and emerging threats are discovered. Good relationships with local law enforcement will also provide warnings when there are events taking place that could affect the security of the substation.

Delay

Delaying criminals or other nefarious actors attempting to access the electrical substation will assist responding security patrols or law enforcement with identifying and possibly apprehending the perpetrator.

Recover

Recovery from an incident is an important consideration for decision-makers when determining if a site warrants additional resources. If a site provides electrical service to a large metropolitan area or there are hospitals that are major trauma centers for an area, the need for uninterrupted electrical service is very high. At the very least, decision-makers should determine what would be needed in the interim should an electrical substation suffer an incident that interrupts power distribution for an extended period of time.

Electrical Companies: Positive Control of Access to Substations, Understanding the Current Threats Using Trend Analysis, Risk Analysis Skills

To expand further on assessing criticality, vulnerability, and risk to an electrical substation, the CARVER acronym will be used. The following table will provide an example of an assessment of a hypothetical electrical substation that includes a score of 1-10 for each area.

Criticality	8	Very critical as it provides service to a large city.
Accessibility	6	Walls are installed and CCTV is installed and operational. No IDS; however, Law Enforcement patrols often.
Recuperability	2	Some ability to recover in the short term, however, if the damage is substantial no interim solutions are available.
Vulnerability	6	Good physical security is in place. However, the site is located in a low area that could be susceptible to flooding.
Effect	8	The loss of this substation would have a significant effect on the local area that this substation provides electricity to.
Recognizability	10	This is a large substation with powerlines coming to and going out of- so it is obvious that it is an electrical substation.

(Source: Food and Drug Administration, 2018)

Once the CARVER matrix has been completed, the next step is to conduct a Risk Assessment for each of the types of threats that the substation could be susceptible to (e.g., theft, vandalism, attack, vehicle crash, flooding, etc.). A simple calculation is Threat (T) multiplied by Criticality (C) multiplied by Vulnerability (V) equals Risk, FEMA uses the term "Asset Value" instead of Criticality; however, for the purpose of this research and for simplicity- Criticality will be used (FEMA, 2004). Here is an example using the same hypothetical electrical substation that the CARVER assessment was completed shown above.

Threat Type	T Score (x)	C Score (x)	V Score (=)	Risk Score	Notes
Flooding	8	8	8	512	Low lying area that has flooded
Theft	6	8	4	192	Ladder could be used for wall CCTV on Site
Rifle Attack	4	8	2	64	Walls in place CCTV on Site
Vehicle Crash	4	8	2	64	Not located near any roadways- limited risk

In the case of this hypothetical electrical substation, the highest risk that should be addressed is the risk of flooding. This information will assist decision-makers with allocating

funding to address the flooding concerns. This process, CARVER, and Risk Assessment would then be completed on all of the substations that are owned by the utility company. Also, as the threats change, or new threats emerge- new assessments should be completed. At a minimum, fencing, signage, and lighting should be installed at any substation. The signage could be the standard, "No Trespassing," or provide notice that the property is under video surveillance. Secondary means of communication for any alarm systems would be beneficial- in the Metcalf incident, the communication lines were disabled.

Local Law Enforcement: Partnership with Utility Companies, Understanding Limited Patrol Capabilities of Substations, Communication with the Community

The availability of law enforcement to respond to a possible incident is an important consideration. The utility company should establish a good relationship with local law enforcement. This will not only provide the utility company with current crime trends in the area but also assist the leadership of law enforcement in understanding how important the uninterrupted supply of electricity is to their community. If law enforcement is not able to adequately respond to incidents at these electrical substations' sites, the use of private security should be considered. In either case, local law enforcement partnerships will assist in current and future assessments.

An additional consideration for decision-makers is future construction or development in the area that could either improve the area around the substation or cause new threats or vulnerabilities to emerge. Again, this is why the continual practice of conducting assessments is so important. The key is to use a consistent process for conducting assessments that is objective, repeatable, and easily understandable.

When determining which threats should be considered, it is important to define them as Possible, Plausible, and Probable. In an article, van der Helm explains these as, “Probability refers to concepts of chance and likeliness… Possibility refers to a claim of reality, whether some future either can be or cannot be (and nothing in between)... Plausibility refers to the structure of the argument, where truth-value is based on the convincingness, the credibility, of the discourse describing the future” (2006). When looking at types of threats, anything is possible, which means that there would be too many possibilities. Plausible threats are realistic threats, but to filter these vast threats further down to actionable countermeasures, the focus must be on the threats that will probably happen.

Local Community Awareness Suggestions

In the event that local law enforcement is not able to take on the additional workload of actively patrolling the electrical substation sites and private security patrols are not a long-term option, another resource that can be utilized are the customers in the areas adjacent to the sites.

Explaining the Limitations of Physical Security and Law Enforcement

In order to assist these customers, an explanation of the limitations of both the physical security of the site and the demands that are placed on law enforcement should be explained. There is a program called the Threat Liaison Officer currently in place in the state of Colorado through the Colorado Information Analysis Center. “The program was developed to provide participants with effective means of information sharing related to local, regional, and global threats, suspicious activity and large-scale incidents” (2022). This program is already established and provides training to participants.

Suggested Reportable Incidents "See Something Say Something"

Another established program through the Department of Homeland Security (DHS) is the "If you See Something, Say Something" (2022). The list of reportable suspicious activity includes the following activities that would pertain to electrical substations, "Surveillance… Theft/Loss/Diversion… Testing or Probing of Security… Breach/Attempted Intrusion… Sabotage/Tampering /Vandalism… Sector-Specific Incident…" (DHS, 2022). Emphasis on the details that civilians should provide is important- as accurate information helps investigators.

Proposal of Incentives for Customers that Report Suspicious Activity

The last recommendation is the use of incentives for customers that agree to take an active role in the security of the electrical substations that provide electricity to their businesses, homes, etc. In an effort to encourage this participation, utility companies could offer a discount on the current utility bill for a customer that observes a suspicious incident and reports the incident to law enforcement. The key is that the customer is only there to observe and get detailed information on the perpetrator(s) description and specific information about the vehicle used (e.g., make, model, color, license plate, etc.). These customers should not attempt to intervene, only observe and report.

Conclusion

The protection of critical infrastructure is essential to the consistent power supply needed for communities to continue to maintain productivity and societal norms. While this research focused on electrical power substations, the methods and principles listed can be utilized for other aspects of critical infrastructure. The key is consistently using the same methods and rating scales when conducting risk assessments. Through these assessments, decision-makers are provided with realistic options that can counter current threats to these substations.

Through the use of an “All Hazards” approach to risk assessments, threats are identified, and countermeasures can be put in place to mitigate these threats (ready.gov, 2021). There will, of course be costs associated with these countermeasures and by conducting risk assessments on all of the substations that will assist decision-makers with prioritizing which substations should receive funding for these countermeasures initially and which will receive funding in the future.

The theories addressing criminal behavior highlighted in this research are just a few of the possibilities currently available. There will likely be new and innovative theories in the future that could provide insights and solutions for preventing crime. Whether the perpetrator is motivated to commit theft, vandalism, or terrorism, the countermeasures are similar in that they are put in place to deter these actors.

There are many examples of vulnerability and risk assessments currently in use in various countries that specifically address critical infrastructure. Some of these utilize methodologies that are complex and often use mathematical equations that could be confusing when presented to decision-makers. The formula of Threat (T) multiplied by Criticality (C) multiplied by Vulnerability (V) equals Risk, which is based on an example from FEMA (2004), provides a simple solution to simplify this complicated methodology. It is important to note that this is a way, not the only way, to provide a useful assessment of vulnerabilities and, ultimately the risks to a substation.

Simply putting countermeasures in place at these substations is not a complete solution to protecting these components of critical infrastructure. What is needed is the assistance of the local community. Whether it is the businesses in the area collocated with the substation or the local law enforcement that is responsible for responding to an incident that occurs, the

relationship between the utility company and these local stakeholders is key to the overall protection of these substations.

The future demands on the electrical power grid are just beginning to be understood. As more electric vehicles are purchased, the need for uninterrupted electrical power will become even more critical. Currently, there are states that have issues meeting the current electricity needs of their citizens, especially during the summer when demands for air conditioning significantly increase in many regions of the United States.

Whether the incentive is to increase the supply of reliable electricity at the local, state, or federal level; improvements to this segment of the critical infrastructure of the United States assist with the overall National Security of the country. Often, citizens focus on their own electricity needs- providing warmth or cooling, cooking, lighting, and refrigeration; however, if electrical power is interrupted for an extended period of time, citizens realize just how reliant they are on electricity.

As stated at the beginning of this research paper, electrical power substations are critical as they are a single point of failure to electrical service in the area they provide service. The challenge lies with balancing the cost of securing these sites, with additional security patrols or significant improvements to the physical security of the substation, compared to the perceived risk of a human-caused attack as well as the effect on the community if electrical service is interrupted.

Limitations of the Research

There are limitations to the research utilized for this paper. As noted by Kitagawa et al., The United Kingdom and the United States government view Critical Infrastructure Protection as

classified information, and therefore, the civilian population is not well informed on the risks and threats to Critical Infrastructure in their respective country (2017). As such, there is limited information and peer-reviewed articles that address the needs of the infrastructure in these countries. Research is likely being conducted. However, it is likely at the government level- either state or federal.

It is also likely that utility companies have completed research and compiled data on actual incidents that have caused damage to their respective electrical components. Again, the sensitive nature of this information could, understandably, make these companies apprehensive with respect to sharing the information with the public.

There are certain topics and specifics that were only briefly discussed as they could be used to increase the effectiveness of some criminal actors- because of this, generalities were used in some instances. The focus was on actual incidents reported in the news or using examples of threats addressed in assessments of critical infrastructure in other countries referenced in the peer-reviewed articles referenced throughout this paper.

As stated in this research paper, the suggested guidelines are just that, a guide that utility companies could use to develop a course of action to correct or reduce these risks; it is not a blueprint that can be used in a "cookie-cutter" approach. As new and emerging threats arise, utility companies must adapt and incorporate innovative ideas to counter these threats. It is also important to consider the threats that could come from within the organization- this could include a disgruntled employee that is willing to cause damage to the utility company.

Recommendations for Future Research

In the future, it could be recommended that best practices be shared that illustrate the effectiveness of physical security currently employed at substations throughout the United States.

However, as this type of information could still be considered classified in the United States, the information may have to be collected in other countries. At the very least, this information should be collected and shared privately within the Critical Infrastructure industry as a way to increase the overall resilience of the electrical power grid. If this information is designated as classified and not meant to be shared with the general public, at least the utility companies would have access to it.

Additionally, utility companies should work with emergency management agencies at the state level to increase information sharing on the current threats that could affect the electrical power supply. This type of partnership could assist with not only human-caused threats but also natural threats. In addition, working with local law enforcement and significant stakeholders in the local community could provide additional insights. The establishment of the Threat Liaison Officer program, similar to what is established in the state of Colorado, is another opportunity to collect future research.

Any future research will depend on the quality of information that is being collected. The increased awareness, at the local and state level, of the threats to electrical substations should lead to more suspicious activity being reported. Ultimately, this should lead to an increase in the number of crimes being prosecuted. This type of information should be collected and categorized for future reference.

References

Baggott, S. & Santos, J. (2020). *A risk analysis framework for cyber security and critical infrastructure protection of the U.S. electric power grid*. Risk Analysis, Vol. 40

Ball, K. (2022). *Electrical substation vandalized causing thousands to lose power*. Retrieved April 19, 2022, from: https://www.kxii.com/2022/03/11/electrical-substation-vandalized-causing-thousands-lose-power/

Baloye, D. & Palamuleni, L., G. (2017) *Urban critical infrastructure interdependencies in emergency management*. Disaster Prevention and Management Vol. 26 No. 2, 2017 pp. 162-182

California Air Resource Board. (2022) *California moves to accelerate to 100% new zero-emission vehicle sales by 2035.* Retrieved September 6, 2022, from https://ww2.arb.ca.gov/news/california-moves-accelerate-100-new-zero-emission-vehicle-sales-2035

Center for Problem-Oriented Policing. (2022). *Situational crime prevention*. Retrieved September 27, 2022, from: https://popcenter.asu.edu/content/situational-crime-prevention-0

College of Policing. (2022). *What is situational crime prevention?* Retrieved September 27, 2022, from: https://www.college.police.uk/guidance/neighbourhood-crime/what-situational-crime-prevention#:~:text=Situational%20crime%20prevention%20focuses%20on,occur%20(Clarke%2C%201997).

Colorado Information Analysis Center. (2022). *Threat liaison officer program*. Retrieved October 13, 2022, from: https://ciacco.org/default.aspx?MenuItemID=63&MenuGroup=Public+Home&AspxAutoDetectCookieSupport=1

Department of Homeland Security. (2022). *If you See Something, Say Something: Recognize suspicious activity*. Retrieved October 13, 2022, from: https://www.dhs.gov/see-something-say-something/recognize-the-signs

Department of Justice (2022). *3 men plead guilty to domestic terrorism crime related to plans to attack power grids.* Retrieved May 5, 2022, from: https://www.justice.gov/usao-sdoh/pr/3-men-plead-guilty-domestic-terrorism-crime-related-plans-attack-power-grids

Dick, K., Russell, L., Souley-Dosso, Y., Kwamena, F. & Green, J., R. (2019). *Deep learning for critical infrastructure resilience.* American Society of Civil Engineers.

Elkabets, S. M. & Shohet, I. M. (2015). *Resilience Modeling (TRA) for critical infrastructures to withstand extreme events-sensitivity analyses.* In Proceedings of the Creative Construction Conference, Krakow, Poland, 21–24 June 2015.

FEMA. (2004). *Unit V - Risk Assessment / Risk Management.* Retrieved October 11, 2022, from: https://www.fema.gov/pdf/plan/prevent/rms/155/e155_unit_v.pdf

Food and Drug Administration. (2018). *An overview of the CARVER plus shock method for food sector vulnerability assessments*. Retrieved April 19, 2022, from: https://www.fda.gov/food/food-defense-programs/carver-shock-primer

Google Maps. (2022). *Screenshot of Google Maps Streetview*. Retrieved October 4, 2022, from: https://www.google.com/maps/@43.0296896,-88.0571449,3a,15y,94.79h,90.86t/data=!3m6!1e1!3m4!1soJ7JgrrTxlBQN2IVF4OGQw!2e0!7i16384!8i8192

Große, C. (2021). *Multi-Level planning for enhancing critical infrastructure resilience against power shortages—An analysis of the Swedish system of STYREL.* MDPI

Haddow, G., Bullock, J., & Coppola, D. (2021). *Introduction to emergency management* (7th ed.). 405. Elsevier Inc.

Huff, J., Medal, H. & Griendling, K. (2018) *A model-based systems engineering approach to critical infrastructure vulnerability assessment and decision analysis.* Wiley Periodicals, Inc.

Huisman, W. & van Erp, J. (2013). *Opportunities for environmental crime: A test of situational crime prevention theory.* Oxford University Press. pp. 1178–1200

Kaplan, S., & Garrick, B. J. (1981). *On the quantitative definition of risk.* Risk Analysis, Vol. 1, No. 1, 11–27.

Kitagawa, K., Preston, J. & Chadderton, C. (2017). *Preparing for disaster: a comparative analysis of education for critical infrastructure collapse*. Journal of Risk Research, 2017 Vol. 20, No. 11, 1450–1465.

Kosowski, B. (2019) *Critical infrastructure in the national security system.* SFT Vol. 54 Issue 2, 2019, pp. 132–141

Mihinjac, M., & Saville, G. (2019). *Third-Generation crime prevention through environmental design*. MDPI

Muhyi, M.M., Gabe, R.T., & Adianto, J. (2019). *Defensible space in urban housing in Indonesia*. IOP Conf. Series: Materials Science and Engineering 523

Nuclear Regulatory Commission, (2020). *Physical protection*. Retrieved April 19, 2022, from: https://www.nrc.gov/security/domestic/phys-protect.html

Olausson, P.M. (2019). *Planning for resilience in the case of power shortage: The Swedish STYREL policy*. Sciendo.

Phillips, S. (2019). *Federal regulation for a "resilient" electricity grid*. Ecology Law Quarterly, *46*(2), 415–454.

Piroozfar, P., Farr, E. R. P., Aboagye-Nimo, E., & Osei-Berchie, J. (2019). *Crime prevention in urban spaces through environmental design: A critical UK perspective*. Elsevier Ltd

Ready.gov. (2021). *Planning.* Retrieved September 6, 2022, from: https://www.ready.gov/planning

Riverside California. (2016). *Outage types*. Retrieved September 19, 2022, from: https://riversideca.gov/utilities/outage-types

Stout, S., Lee, N., Vogel, J., Giangola, L., & Leisch, J.(2020). *Lao power sector vulnerability assessment and resilience action plan*.

United States Air Force. (2018). *Air force policy directive 31-1*. Retrieved May 5, 2022, from: https://static.e-publishing.af.mil/production/1/af_a4/publication/afpd31-1/afpd31-1.pdf

United States Air Force (2019). *Air force doctrine 3-10*. Retrieved September 6, 2022, from: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-10/3-10-D10-FORCE-Risk-MGMT-Process.pdf

USAF Police Alumni Association. (2021). *Security Specialist.* Retrieved October 11, 2022, from: https://www.usafpolice.org/security-specialist.html

Van der Helm, R. (2006). *Towards a clarification of probability, possibility and plausibility: how semantics could help futures practice to improve*. Consortium for Science Policy and Outcomes, at Arizona State University. Retrieved October 11, 2022, from: https://cspo.org/wp-content/uploads/2014/11/read_van-der-Helm-Towards-a-Clarification-of-Probability.pdf

Vogiatzaki, M., Zerefos, S., & Tania, M.H. (2020). *Enhancing city sustainability through smart technologies: A framework for automatic pre-emptive action to promote safety and security using lighting and ICT-based surveillance*. MBPI

Vogt, D. (2022). *Elizabethtown police seek suspects who stole, damaged equipment from electrical substation*. Retrieved April 19, 2022, from: https://www.wave3.com/2022/03/23/elizabethtown-police-seek-suspects-who-stole-damaged-equipment-electrical-substation/

Yao, X., Wei, H., Shohet, I. & Skibniewski, M. (2020). *Assessment of terrorism risk to critical infrastructures: The case of a power-supply substation*. MDPI

Appendix

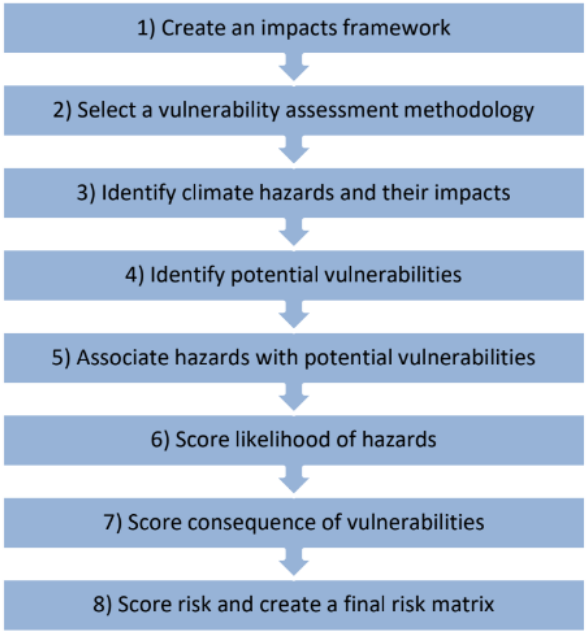


Figure 1. Vulnerability Assessment process

Source: Stout et al., 2020

Table 2. Subset of Potential Vulnerabilities Associated with a Subset of Hazards from a VA of the Lao PDR Power Sector

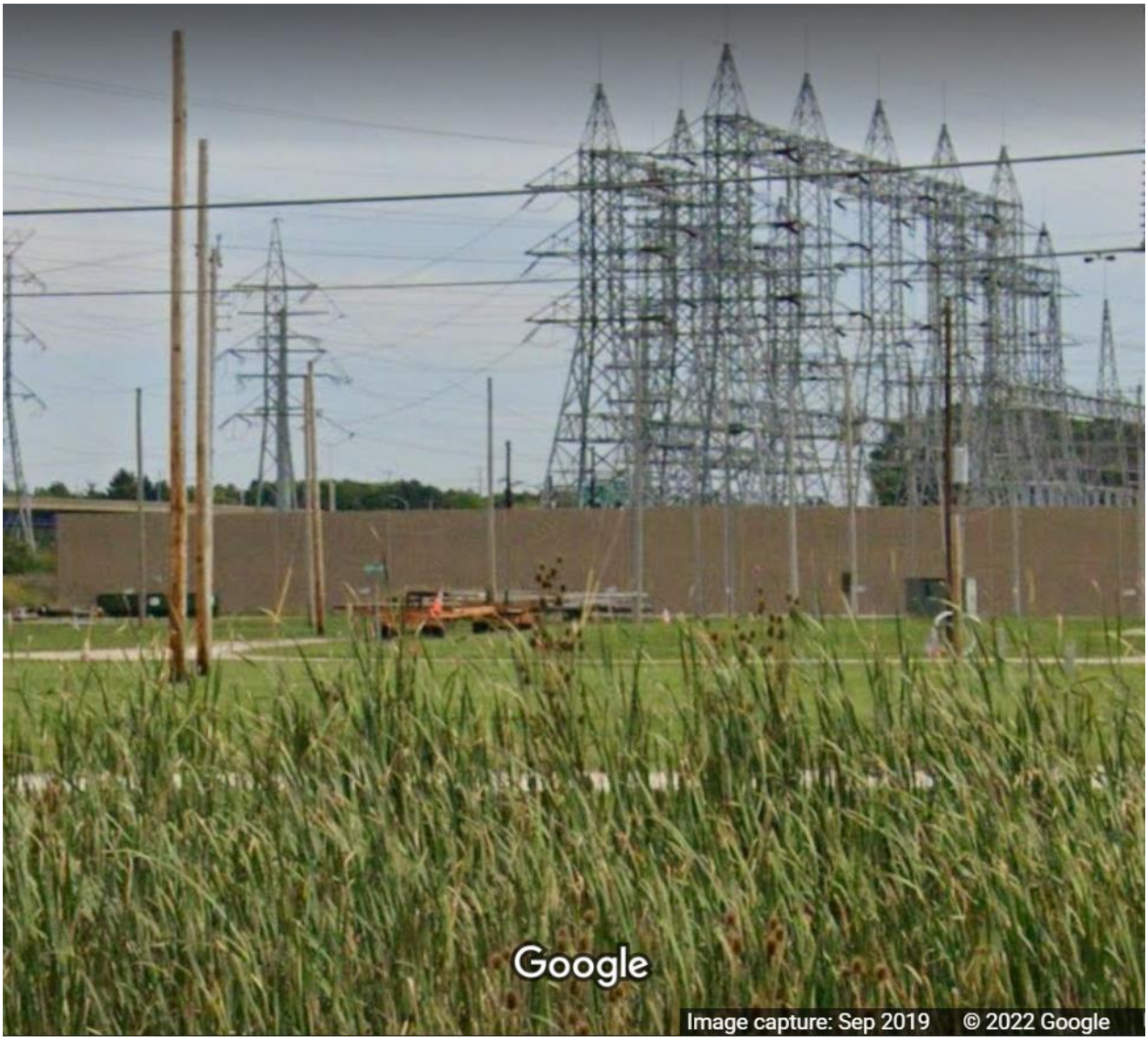
Hazards	Vulnerabilities					
	Power system rules, regulations, and technical standards do not meet current and changing environmental conditions	Corruption leads to code violations	Dam construction does not follow design specifications	Installation does not follow design specifications	Lack of compliance with codes in design	System operations are not flexible enough to respond to changes in demand and supply
Extreme Precipitation	Yes	No	Yes	Yes	Yes	Yes
Extreme Temperatures	Yes	No	No	No	No	Yes
Flooding	Yes	No	Yes	Yes	Yes	Yes
Landslides	Yes	No	Yes	Yes	Yes	No
Wildlife Interactions	No	No	No	No	No	No
Wind	Yes	No	No	No	No	Yes
Human Actions: Bad Actors	No	Yes	Yes	Yes	No	No
Human Actions: Accidents	No	No	Yes	Yes	No	No
Technological Design	Yes	No	Yes	Yes	Yes	Yes

Source: Stout et al., 2020

TABLE 3 Timeline of Metcalf attack[32]

Time	Description of event
12:58 AM	AT&T fiber-optic telecommunications cables were cut—in a way that made them hard to repair—in an underground vault near the substation, not far from US Highway 101 just outside south San Jose.
1:07 AM	Some customers of Level 3 Communications, an Internet service provider, lost service. Cables in its vault near the Metcalf substation were also cut.
1:31 AM	A surveillance camera pointed along a chain-link fence around the substation recorded a streak of light that investigators from the Santa Clara County Sheriff's office think was a signal from a waved flashlight. It was followed by the muzzle flash of rifles and sparks from bullets hitting the fence. The substation's cameras weren't aimed outside its perimeter, where the attackers were.
Approximately 1:37 AM	PG&E confirms it got an alarm from motion sensors at the substation, possibly from bullets grazing the fence, which is shown on video.
1:41 AM	The sheriff's department received a 911 call about gunfire, sent by an engineer at a nearby power plant that still had phone service.
1:45 AM	Riddled with bullet holes, the transformers leaked 52 000 gallons of oil, then overheated. The first bank of transformers crashed and PG&E's control center about 90 miles north received an equipment failure alarm.
1:50 AM	Another apparent flashlight signal, caught on film, marked the end of the attack.
1:51 AM	Law-enforcement officers arrived, but found everything quiet. Unable to get past the locked fence and seeing nothing suspicious, they left.
2:03 AM	PG&E's control center called a worker to go to the Metcalf site.
3:15 AM	A PG&E worker arrived at Metcalf to survey the damage.

Source: Huff et al., 2018



Source: Google Maps Streetview, 2022