infrastructures

MDPI

Article

Will Updated Electricity Infrastructure Security Protect the Grid? A Case Study Modeling Electrical Substation Attacks

Jenna K. McGrath

School of Public Policy, Georgia Institute of Technology, Atlanta, GA 30332, USA; mcgrathj@gatech.edu

Received: 18 September 2018; Accepted: 17 November 2018; Published: 20 November 2018

Abstract: As targeted attacks continue to threaten electricity infrastructure, the North American Electricity Reliability Corporation (NERC) and private utilities companies are revising and updating the physical and cybersecurity standards for grid infrastructure in the United States (U.S.). Using information collected about past physical attacks, feasible physical and cyber-physical attacks are modeled against the proposed updated security standards for a U.S.-based generic electric substation. Utilizing the software program Joint Conflict and Tactical Simulation (JCATS), a series of increasingly sophisticated physical attacks are simulated on the substation, as are a set of cyber-enabled physical attacks. The purpose of this study is to determine which of the security upgrades will be most effective at mitigating damages to the electrical infrastructure from an attack. The findings indicate that some of the utility and agency-proposed security measures are more effective than others. Specifically, additional barriers around the substation and physical armored protection of transformers are most effective at mitigating damages from attacks. In contrast, increased lighting at the substation and reducing the surrounding foliage are not as effective. This case study demonstrates a modeling analysis approach to testing the efficacy of physical security measures that can assist in utility and agency decision-making for critical infrastructure security.

Keywords: critical infrastructure; electric grid; physical attack; cyber-enabled attack; resilience

1. Introduction

The electricity infrastructure in the United States (U.S.) is not only vulnerable to weather events, technical and human errors, but also to malicious, intentional attacks [1]. This vulnerability has been evident for decades; between 1970 and 2017, there have been approximately 527 suspected and confirmed physical attacks on grid infrastructure [2,3]. While cyberattacks are reported less frequently and are more difficult to confirm, there have been at least 20 confirmed attacks since 2002 [2,3]. Given the vastness and age of the U.S. electricity infrastructure, it is difficult to maintain advanced security across all sites. However, in recent years there has been more of an effort from both the federal government and utility operators to improve physical and cyber security, with enhancements tending to start at the most vulnerable and critical sites.

One of the more publicized and costly physical attacks on the grid occurred in 2013 at the Metcalf Power Station, located near San Jose, California. This attack, which resulted in $15 million in damages and required the substation to be shut down for three weeks while initial repairs took place [4], served as a catalyst for a series of attack mitigation strategies aimed at improving grid security. To prevent a similar attack from happening again, utility companies and the North American Electricity Reliability Corporation (NERC) outlined a range of security improvement measures, including more robust physical barriers around key infrastructure, additional security technology and security personnel on site, and new risk mitigation audits to identify and communicate about vulnerabilities amongst sites [5].

The overarching motivating question, to be addressed here, is how successful the security improvements proposed by utilities and NERC will be at preventing attacks. Given what is known about past attack methods and what is suspected for potential attacks, will the security improvement strategies adequately mitigate future threats? To answer this question, a review of literature is first described. Next, existing and proposed security standards, and data and information collected from the nearly 500 past physical and cyberattacks (paying particular attention to the 2013 Metcalf attack) are used to model increasingly sophisticated attacks, including cyber-enabled physical attacks, against multiple security level scenarios. The attack scenarios are modeled in the Joint Conflict and Tactical Simulation (JCATS) software program, developed by Lawrence Livermore National Laboratory (LLNL) and used to simulate the outcomes of user-defined data [6]. A discussion of the results and research contributions follow, concluding with directions for future research.

1.1. Literature Review

Resiliency, reliability, and security of the United States' critical infrastructure sectors, particularly the electricity and energy sector, is a focus of concern for the government, industry, and academics alike. After conducting an in-depth report in 2007 regarding electricity infrastructure vulnerabilities, the National Research Council of the National Academies pushed to have the report released to the public, so as to better inform policymakers and industry experts of the report's findings [1]. In the years since, there has been an increase in federal research and development funding within the Department of Energy's Office of Electricity, which may indicate a renewed focus on maintaining a resilient and reliable electric grid [7]. With the many aging components that comprise electricity infrastructure, investments from utility owners, operators, and regulatory agencies are expected to come in waves [8].

Aside from industry reliability and security standards becoming more rigorous within the NERC (to be discussed in more detail in the following sections), there is a host of research related to risk management and disaster resiliency modeling. Past research in this area has focused on methodologies to develop baseline standards, indicators, and guides to assist in infrastructure and community resiliency standards and risk mitigation strategies. For example, in their 2018 research, Mathias et al. outlined dynamic modeling approaches to help better monitor, inform, and prepare those in charge of critical infrastructure management in the wake of threats [9]. Better communication across stakeholders is often included as an appropriate step in risk management and resiliency planning for natural disasters [10,11], and is seen as a key step in NERC's infrastructure security improvements. Communication is also a focus with the increase in research, development, and deployment of smart grid technologies. While smart grids may present inherent cybersecurity risks given the network connectivity, the implementation of advanced technology on the grid also allows for an increase in automated communication [8]. This means smart grids can incorporate automated risk detection methods and self-healing strategies, in the event of both cyber and physical attacks, as a mechanism by which to maintain uninterrupted flow on the power grid [8]. This automated response can also help address load uncertainty associated with renewable generators [12].

The simulations presented below are based on detailed information of past attacks on the U.S. grid infrastructure. Focusing on past attacker profiles, attack methods, and subsequent damages, the model serves as a case study for a generic electrical substation attack. Given what is known about past attacks, the simulation is aimed at evaluating the potential success past attacks could have had against new security upgrades, as well as to consider what sort of damages from future, more sophisticated attacks, can be anticipated. The overarching question is whether the proposed and implemented security upgrades at grid infrastructure sites will in fact be capable of mitigating or preventing future attacks. Below, the Metcalf attack is outlined, followed by the utility-level security improvements and NERC-level security improvement recommendations that are either proposed or already implemented for electricity infrastructure across the country.

1.2. Metcalf Attack and Utility-Level Security Improvements

The Metcalf attack is instructive not only as a prime example of a successful, modern physical attack, but also as an illustration of the subsequent monetary damages and industry response to improving grid security. The Metcalf power station, owned and operated by Pacific Gas and Electric (PG&E) near San Jose, California, was targeted by an unknown number of attackers early in the morning on 16 April 2013. The assailants first cut underground AT&T telephone communication cables that serviced the station, and then situated themselves just out of view of the power station's security cameras. An attacker shot at the substation, including the station's transformers, with a semiautomatic rifle for just under 20 min. Although a security guard onsite was able to call 911 during the attack from his cell phone, and PG&E received an alert from a motion sensor triggered at the site, the attackers left the area before police arrived and have not yet been identified. While no one was injured, the attack left 17 transformers damaged, costing PG&E $15 million in repairs and shutting down the substation for 21 days (power was rerouted to other substations in the region). The transformers were damaged but not destroyed, leading to debate within the industry and the Federal Bureau of Investigation (FBI) about whether the attackers specifically targeted the transformers or were shooting randomly [13]. Transformers cost approximately $3 million each, so targeting transformers has the potential to result in a costly attack [14].

Perhaps because this attack could have resulted in extremely high repair costs, or perhaps because the attack demonstrated a vulnerability at electricity infrastructure across the U.S., PG&E and other utility operators took notice and initiated security improvements. In December of 2014, PG&E pledged $10 million over three years to improve their critical infrastructure protection for power and substations similar to Metcalf. After being fined $50,000 by the State of California for the theft of $40,000 worth of construction equipment from the Metcalf site, PG&E declared in 2015 an additional $200 million investment for substation security at the most critical and/or most vulnerable facilities across California. Approximately 40 percent of the investment was dedicated for physical barrier security and 60 percent towards technological security improvements [15].

Some of the initial security improvements PG&E focused on included round-the-clock security guards on site (plus additional training for overnight guards) [15], removing foliage and undergrowth that could provide hiding places, improving and increasing lighting onsite, and adding security perimeter and internal fencing (chain link and concrete) [16]. Additional and improved security camera technologies (such as thermal cameras and enhanced detection analytics) are proposed to be added in the future, as well as a gunshot detection system [15]. Other utilities across the country are following suit. Despite not experiencing any publicized attacks on their infrastructure, Virginia Dominion Resources pledged to invest $300 to $500 million in 2014 to improve security at their sites [13].

1.3. NERC-Level Security Improvements

More overarching, however, are the measures NERC has taken to increase awareness of security vulnerabilities and improve information sharing across the NERC regions. First, in January of 2015, the Electric Information Sharing and Analysis Center (E-ISAC) within NERC created the Physical Security Analysis Team (PSAT). The PSAT's mission is to assist NERC members in identifying vulnerable physical security infrastructure and develop new physical security plans. Members receive physical security updates and suggestion bulletins, and information and planning scenario pamphlets. For example, bulletins have focused on installing unmanned aircraft surveillance systems at vulnerable infrastructure, and planning exercises to mimic worst-case scenarios [17]. In addition, in March of 2015, the Physical Security Advisory Group (PSAG) was created to assist in analyzing current and potential physical security threats. Members of PSAG consist of industry experts and representatives from both the Department of Energy and the Department of Homeland Security [17]. NERC views membership participation and communication within the E-ISAC portal to be a critical component in both physical and cyber security improvements (awareness, troubleshooting, security mitigation efforts). One of

the main goals of the group is to have physical and cyber security data and standardization metrics available from a centralized source so all members have access to the same information and incidents are easily shared [17]. NERC's emphasis on communication and information sharing is in line with other research relating to critical infrastructure risk management and disaster resiliency as well [9,11].

The main NERC contribution to improving electricity infrastructure security is the CIP-014-2 standards, requested by the Federal Energy Regulatory Commission (FERC) in March of 2014 and finalized in 2015 [5,18]. The purpose of CIP-014-2 is to protect vulnerable and critical transmission stations and substations from becoming inoperable, damaged, or resulting in a cascading failure as a result of a physical attack [19]. This applies to substations 500 kilovolt (kV) or higher and certain substations between 200 kV and 499 kV that are deemed high priority or critical [5]. NERC outlines six requirements within the CIP-014-2 plan:

1. Owners of transmission stations must provide risk assessments to current and future infrastructure.
2. A third party must verify the risk assessment and provide recommendations for risk mitigation.
3. The risk analysis must then be provided to the managers or operators of said infrastructure.
4. For all of the sites where risk assessments were performed, the owners must then also provide an evaluation and identify vulnerabilities of potential physical attacks.
5. All owners must provide a detailed physical security plan to have on file after the risk assessment is conducted.
    a. The plans should include: Identifying vulnerabilities; outline deterrent and mitigation plans of potential attacks; communication plans, detection techniques; how to contact and coordinate with law enforcement in the event of an attack; provide a timeline of when physical security improvements will be initiated and completed; how to continuously monitor and update security plans given evolving physical threats.
6. A third party is then expected to review the physical security evaluation and resulting plan that is developed. The third party must be certified to conduct physical protection assessments, be from a NERC-approved organization, or be a government agency, law enforcement, or military security expert.

2. Materials and Methods

In this analysis, a substation operating as part of the U.S. electrical grid is created as the site for which all security upgrades are implemented and all attacks take place. Though the substation is fictional and generic, its layout, equipment placement, surrounding environment, and other features are similar to those found at substations across the U.S. The fictional substation is located on the outskirts of a metropolitan area, surrounded by vegetation and with a main road nearby. Each scenario in the analysis occurs at twilight. The targets are the 20 transformers onsite. Transformers are targeted due to their critical role in the delivery of reliable electricity and the fact that they are expensive and difficult to repair and replace, and also because they have been targeted frequently in the past (including the 2013 Metcalf attack) [1].

To model the incremental security upgrades against different attack scenarios, the computer modeling program JCATS is used. JCATS is a program created and maintained by Lawrence Livermore National Laboratory, used to stochastically determine the outcomes of discrete events and actions, with the statistical data to run the scenarios defined by the user [6]. The first steps in building a model in JCATS is to define the problem, conditions, and target types one wishes to model, as well as the defensive and adversary forces. Next, the aims of the attack and tactical information of both the adversary and the defenders are inputted. In building the specific scenarios of the model, details about the terrain, actor behaviors, and tactical information are determined by the user and can be varied [20,21].

While much of the data that is input into JCATS is collected by the user (here, information about past physical and cyberattacks on electricity infrastructure), there are some parameters pre-programmed within the computer software. For example, military field experiments provide specific data outputs for weapon range, visibility, and probability line of sight acquisitions in various lighting and vegetation conditions. Previous research has used JCATS primarily for military-related research, including emergency management and response modeling [22], wargames training to simulate possible outcomes for military troops in various terrain conditions [23], and to provide a risk assessment for potential damages to U.S. ports from maritime improvised explosive devices [24]. The ability for the JCATS computer program to create specific terrain, infrastructure, and conditions allows for users to input the conditions for a disaster, emergency, or attack, including behavior of the actors, weapons, and safety procedures.

In this study, there are two categories of user-defined data: Security upgrade levels and attacker profiles. Security upgrade levels include the baseline security standards currently used at most substations through to the most stringent security standards currently being implemented by utilities. The attacker profiles are three distinct groups of adversaries, ranging from Amateur to Elite, that attack the substation in the model. The data collected and assumptions used to create the user-defined security upgrade levels and attacker profiles are explained below, preceded by description of the site and its environment that is used throughout the simulations.

The security upgrade levels are designed to indicate the physical security improvements to critical grid infrastructure that have been proposed or implemented by grid operators, NERC, or federal and state governments (as described in the previous section). Starting with basic physical security features that most substations already have (noted as "Baseline" in the analysis), four incremental security upgrades ("Security Upgrade 1–4") scenarios show increasingly robust security at the model's substation. A summary of the Baseline and Security Upgrades 1–4 can be seen in Table 1.

Table 1. Security Upgrade Scenarios (laboratory-specific reference number LLNL-TR-746040).

	Baseline	**Security Upgrade 1**	**Security Upgrade 2**	**Security Upgrade 3**	**Security Upgrade 4**
Time of day	Twilight	Twilight	Twilight	Twilight	Twilight
Lighting	Low (Deep Twilight)	Medium (Twilight)	Medium (Twilight)	High (Heavy Overcast)	Extra High (Overcast Sunlight)
Vegetation	High (0.6 probability line of site blocked (PLOSB)	Medium (0.2 (PLOSB)	Medium (0.2 (PLOSB)	Low (0.05 (PLOSB)	Low (0.05 (PLOSB)
Perimeter Details	Chain fence	Chain fence + interior chain fence	Chain fence + interior chain fence	Concrete wall + internal chain fence	Concrete wall + internal chain fence + armored shielding around transformers
Cameras/Motion Sensors	Basic (70% probability of detecting intruder)	Additional Cameras/Sensors (80% probability of detection)	Additional Cameras/Sensors (80% probability of detection)	Advanced cameras + motion sensors weaved into fencing (90% probability of detection)	SU3 features + gunshot detection sensors (100% probability of detection)
Security Presence/Engagement	Two. No patrol, no engagement	Two. No patrol, no engagement	Two, with one patrolling on foot. No engagement	Two, with one patrolling on foot. No engagement	Two, with one patrolling in a vehicle. Engagement
Police Engagement	Yes	Yes	Yes	Yes	Yes

Physical security improvements start with the lighting at the substation and the vegetation surrounding the substation. As noted in the previous section, utilities aim to improve the ability of security cameras and guards to spot potential intruders and threats by increasing the light levels and reducing foliage [16]. The JCATS data that reflects the ability of an attacker to identify and attack a target through different light levels is collected by the U.S. Army Materiel Systems Analysis Activity (AMSAA). Through field experiments, the AMSAA collects acquisition of target and performance data "based on the ACQUIRE type sensor performance and technical data," meaning the troop's ability to acquire and strike a given target in various lighting levels (AMSAA Special Publication No. SP-97,

The Compendium Of Close Combat Tactical Trainer Algorithms, Data, Data Structures And Generic System Mappings. ACQUIRE-TTPM Implementation Guide for Combat Simulations 21 July 2008. Distribution is authorized to U.S. Government Agencies and their contractors: Other requests shall be referred to Director, U.S. Army Materiel Systems Analysis Activity, APG, MD 21005-5071). While the time of day is "twilight" during all scenarios in the model, lighting at the substation improves from "low" (twilight with shadows) in the Baseline to "extra high" (overcast sunlight) in Security Upgrade 4.

Field experiments determine the probabilistic attenuation for line-of-sight, meaning "the probability of acquiring a target in (or through) a feature depends on how far into (or through) the feature an observer has to look." The model assumes that the substation is surrounded by vegetation, and security improvements reduce the probability line-of-site blocked (PLOSB) from "high" (0.6 PLOSB) in the Baseline to "low" (0.05 PLOSB) in Security Upgrades 3 and 4 (assuming there will always be a tree or boulder in the area, modeled vegetation is never reduced to 0 PLOSB).

Additional security features include physically securing the perimeter, securing the transformers, and improving and/or increasing the range of security cameras, motion sensors, and gunshot detection sensors. In the Baseline scenario, the substation is surrounded by a single chain-link fence. As security improvements increase incrementally, additional chain-link fences or concrete walls are erected (Security Upgrades 1–3) with the goal of armored shielding around the transformers (Security Upgrade 4). For security cameras, motion sensors, and gunshot detection sensors, probability of detection is used as an indicator to measure the technological improvements, increase in number, and increase in range of the equipment. However, it must be noted that cameras in areas with relatively high traffic (cars, pedestrians, wildlife) tend to only focus at the immediate 10-foot range surrounding the exterior fence around the site, and motion sensors will only react when disrupted Lawrence Livermore National Laboratory, Global Security Program, personal communication, 30 January–1 February 2018). In the Baseline, cameras and motion sensors have a 70% probability of detecting an intruder, increasing to 90% in Security Upgrade 3. In Security Upgrade 4, probability of detection is increased to 100% due to the addition of gunshot detection sensors, which are assumed to be one of the higher tiers of physical security upgrades a utility may implement.

Responding security and police are included in the security upgrade scenarios. Based on knowledge of existing electrical substation security and the intended security improvements, it is assumed that there will always be two security guards onsite. At the Baseline and in Security Upgrade 1, both security guards remain in the security booth. In Security Upgrade 2 and 3, one security guard is patrolling on foot, increasing the time the guard can detect and report an attack. In Security Upgrade 4, a guard is patrolling in a vehicle, further increasing the detection and reporting time. Only in Security Upgrade 4 do the responding guards engage with the attackers.

2.1. Attacker Profiles

Three distinct attacker profiles are created to demonstrate the varying extent of damages that can be inflected upon grid infrastructure depending on the training and determination of the assailants. These three attacker profiles are Amateur, Trained, and Elite. The distinction between the three profiles is based on examples and knowledge gained from past grid attacks. Incidents of sabotage without planning or an understanding of how the targeted infrastructure operates are classified as Amateur incidents. For example, incidents in which the assailant has manually tried to unscrew bolts of electricity poles or pylons are considered Amateur attacks [25]. Attacks demonstrating knowledge of the infrastructure and/or methods used to carry out the attack are classified as Trained incidents, such as when a former electrical engineer used thermite to attempt to burn through high voltage power lines [26]. While there has yet to be an Elite attack on the grid, an Elite assailant is considered someone who has been specifically trained to a high standard in both the attack method and the infrastructure operations, components, and weaknesses.

As stated, the JCATS program requires users to input some information and data into the system to create statistical simulations. For the attacker profiles, details about weapon types (semiautomatic rifles modeled after those used in the Metcalf, and basic improvised explosive devices) already existed in the JCATS database. The probability that the attackers hit their target, and the probability that said hit causes damage or destroys the target, is user input. For this model, these probabilities were determined first by using the Metcalf attack as a baseline case study. As mentioned above, given the differing opinions between FBI investigators and industry experts for whether the Metcalf attack was carried out by amateurs or perpetrators with more training [13], the hypothesis in this study is that amateur attackers in the model will damage fewer than the 17 transformers damaged in the actual Metcalf attack, whereas trained attacks in the model will damage more than 17. To fine-tune this hypothesis, military experts at LLNL were consulted. These military experts provided information about hit accuracy, expected damage due to weapon type, and the variations between the attacker profiles compared to police and security forces (Lawrence Livermore National Laboratory, Global Security Program, personal communication, 30 January–1 February 2018). Lastly, the probability estimates in Table 2 were cross referenced with literature discussion of police and security target accuracy, where the estimates were confirmed [27].

Table 2. Attacker Profiles, LLNL-TR-746040.

	Attacker Profiles		
	Amateur	**Trained**	**Elite**
Probability of Hit	85%	96%	100%
Probability of Damage: None	27.5%	23.5%	20%
Probability of Damage: Damaged	72%	74.5%	77%
Probability of Damage: Destroyed	0.5%	2%	3%
Engagement with Security/Police	None	None	Yes
Weapon Details	AK47 7.62 × 39, 150 rounds each, 500 m range	AK47 7.62 × 39, 150 rounds each, 500 m range	AK47 7.62 × 39, 150 rounds each, 500 m range
Explosives Details	None	None	Generic IEDs, set off with timer, 10 m explosive range. Probability: 80% damage, 20% kill
Breach Perimeter	No	No	Yes (1 min to cut fence, 2 min to climb barrier)
Additional Equipment	None	None	Equipment to breach perimeters; Night vision/thermal goggles

Additionally, the military experts provided insight about attacker movements, plans, and interactions with responding security and police forces (Lawrence Livermore National Laboratory, Global Security Program, personal communication, 30 January–1 February 2018). Based on these conversations, as well as information about past physical attacks on the grid as presented in Chapter 2, it is assumed that the goal for Amateur and Trained attackers is to cause as much damage as possible to the infrastructure only. Therefore, in the model simulations, Amateur and Trained attackers flee the scene when security or police respond to the attack. Elite attackers, however, are assumed to be highly trained by a sophisticated group or nation state and to be willing to engage with responding security or police forces in order to continue their planned attack. In the model, onsite security forces do not engage unless shot at first: the LLNL military experts advised that proper protocol for security is to call the local police or SWAT team (Lawrence Livermore National Laboratory, Global Security Program, personal communication, 30 January–1 February 2018). Amateur and Trained attackers flee when

onsite security arrives, but Elite attackers confront responding security officers. The responding off-site police forces do engage with the attackers, meaning the model only shows security and police engagement with the Elite attackers.

2.2. Attack Scenarios

Given the differences between each security upgrade level and the three attacker profiles, there are differences in how each attack scenario in the model plays out. The main differences are outlined below in Table 3. In the Baseline and Security Upgrade 1, the terrain is perfectly flat. Therefore, once a wall is constructed in Security upgrade 3, all attacks would be thwarted due to the attackers being unable to acquire a line of sight to the target. However, it is unlikely that all terrain will be absent of trees, hills, boulders, or other features that one could climb to get a better view of the targets. As such, a 1.5-m hill is added to the terrain in Security Upgrades 3 and 4. This hill represents terrain features (naturally occurring features in the environment or even just standing on top of a vehicle) that could allow for assailants to continue their attacks despite a concrete wall blocking an eye-level line of site.

The next set of details that varies for the attack scenarios is how the assailants act. The Amateur and Trained attackers never breach the perimeter of the substation during any attack scenario, therefore they never trigger security cameras. This is because for a substation such as this, situated just outside of a metropolitan area, the activity and traffic nearby is enough to require that cameras only be situated to cover ten feet outside the exterior fence; otherwise passing cars, pedestrians, and animals may constantly trigger the camera's activity alerts (Lawrence Livermore National Laboratory, Global Security Program, personal communication, 30 January–1 February 2018.). The motion sensors will eventually be triggered in each Security Upgrade scenario for the Amateur and Trained attackers, as some of the shots fired will hit the exterior fencing (where motion sensors are located) (Lawrence Livermore National Laboratory, Global Security Program, personal communication, 30 January–1 February 2018.), such as was the situation during the Metcalf substation attack. While security guards are in the guard booth onsite in the Baseline and Security Upgrade 1 scenarios, in the final Security Upgrade (Level 4), gunshot detection sensors are installed, meaning that security guards onsite are alerted to an attack even quicker.

Table 3. Attack Scenario Details.

		Attack Scenario Details				
		Baseline	**Security Upgrade 1**	**Security Upgrade 2**	**Security Upgrade 3**	**Security Upgrade 4**
Attacker Profile:	**Amateur**	Never breaching perimeter, so never triggering cameras, eventually gun shots will trigger motion sensors.		Foot patrolling security guard lead to quicker reaction time in SU2-3		Gunshot detection sensors triggered. Guard patrolling in vehicle.
	Trained					
	Elite	One attacker is always breaching perimeter to place IEDs, so always triggering cameras/motion sensors based on probability of detection (listed in Table 1)				
		-		Foot patrolling security guard lead to quicker reaction time in SU2-3		Guard patrolling in vehicle.
Response Time:	**Security**	Recognize: 5 min React: 5 min	Recognize: 5 min React: 5 min	Recognize: 1 min React: 1 min	Recognize: 1 min React: 1 min	Recognize: 0.5 min React: 0.5 min Arrive: 2 min
	Police	Travel time to arrive at the substation is always 10 min				
	Additional Notes	Flat terrain			1.5 m hill added to environment to demonstrate terrain variability	

Lastly, the time it takes for security and for police to respond to the threat varies for each Security Upgrade. Three factors contribute to the response time: The time it takes for onsite security to recognize that an attack is taking place (based on cameras, sensors, or hearing or seeing an attack themselves), the time it takes the onsite security to react (identifying the location of the attack, the nature of the attack, notifying off-site police), and the time it takes for off-site police (or SWAT) forces to arrive. It is assumed that once onsite security places the call for police response, the time to travel to the substation will always take 10 min, regardless of security upgrade level. As mentioned previously, the Amateur and Trained attackers do not engage with security or police forces, but Elite attackers do. Therefore, in Security Upgrade 4, the onsite security guard patrolling in a vehicle responds to the situation unfolding and upon arrival to the scene, engages with the attacker who breached the perimeter to place improvised explosive devices (IED).

3. Results

3.1. Physical Attacks

Each Security Level Upgrade scenario is run against the three attacker profiles in "batches," meaning JCATS cycles through each scenario 100 times each in order to produce a statistical probability of the outcomes. The baseline substation model in JCATS is shown in Figure 1 (with the attackers red, security blue, and police vehicle blue) and the results are displayed below in Table 4 and Figure 2. The outcomes of interest are the expected average number of "targets" damaged or destroyed by firearms and IEDs in each scenario. For all scenarios, the first target assessed is the average number of transformers (out of 20 total on site) damaged or destroyed in each attack scenario. For the Elite attacker scenarios, the average number of transformers damaged and destroyed by the three IEDs placed onsite is also recorded. As discussed previously, the Amateur and Trained attackers flee once onsite security or offsite police arrive to the scene of the attack, therefore there is never any engagement between the two groups. However, the Elite attackers do engage with responding security and police, with the attackers always shooting first. This engagement means that Elite attackers, security guards, and police officers are also "targets" assessed as damaged or destroyed in the model within the Elite Attacker scenarios.

Figure 1. Baseline Model of Substation in JCATS, LLNL-PRES-746039.

Using the 2013 Metcalf attack and information about other past physical attacks on electricity infrastructure as a guide, the Baseline Security Level Upgrade scenario performs in the expected range of damaged and destroyed transformers. While the Metcalf attack resulted in 17 damaged transformers, the Amateur attackers perform less successfully, with 15 transformers damaged and fewer than one transformer destroyed, on average. The Trained attackers fair better, with nearly 15 transformers damaged and at least four destroyed, on average, indicating that those trained more extensively with the attack weapons will have a better chance of destroying the target. The Elite attackers damaged and destroyed transformers with both firearms and IEDs, but the total count throughout all security upgrade scenarios is not exceedingly high due to one Elite member spending time breaching the perimeter and placing the explosives before beginning to fire upon the substation. There is no engagement between security or police in the Baseline because the guards stay in their booth and the attack concludes before the responding officers arrive.

Table 4. Physical Attack Scenario Results, LLNL-TR-746040.

Security Level	Attacker Profile	Target	Damaged by Firearms	Destroyed by Firearms	Damaged by IEDs	Destroyed by IEDs
Baseline	Amateur	Transformer	15.46	0.93	-	-
	Trained	Transformer	14.9	4.4	-	-
	Elite	Transformer	10.86	3.67	2.52	0.48
		Elite Attackers	0	0	0	0
		Security Guards	0	0	0	0
		Police	0	0	0	0
Security Upgrade 1	Amateur	Transformer	10.54	0.99	-	-
	Trained	Transformer	8.07	3.78	-	-
	Elite	Transformer	7.97	3.4	2.32	0.68
		Elite Attackers	0	0.99	0	0
		Security Guards	0	0	0	0
		Police	0	0	0	0
Security Upgrade 2	Amateur	Transformer	10.86	0.74	-	-
	Trained	Transformer	7.82	4.03	-	-
	Elite	Transformer	7.77	3.6	2.35	0.65
		Elite Attackers	0	0	0	0
		Security Guards	0.26	0.43	0	0
		Police	0	0	0	0
Security Upgrade 3	Amateur	Transformer	15.97	0.79	-	-
	Trained	Transformer	9.94	4.3	-	-
	Elite	Transformer	9.37	4.31	2.35	0.65
		Elite Attackers	0	0	0	0
		Security Guards	0.37	0.4	0	0
		Police	0	0	0	0
Security Upgrade 4	Amateur	Transformer	0.71	0	-	-
	Trained	Transformer	5.13	0.14	-	-
	Elite	Transformer	2.61	0.08	1.11	0.23
		Elite Attackers	0.13	1.18	0	0
		Security Guards	0	0	0	0
		Police	0	0	0	0

In the subsequent Security Level Upgrades, vegetation is reduced and lighting increased, as are the numbers of cameras and sensors. In Security Upgrade 1, interior chain link fences are added around the transformer area, in addition to the perimeter chain fence. This reduces the line of site

for the attackers to acquire the targeted transformers, reducing the average number of transformers damaged and destroyed by all three attacker profiles. Furthermore, even though the response time does not change from the Baseline, the additional chain fence that the Elite attacker must cut through to place the IEDs means that the attack is slowed enough to the point where there is engagement between the Elite attacker and the responding police forces. The Elite attacker is destroyed (i.e., "killed") almost 100 percent (0.99) of the time during the attack scenario.

Security Upgrade 2 proceeds similarly, with the only upgrade in security from Level 1 to 2 being that there is a security guard patrolling on foot. The patrolling officer is able to reduce the amount of time it takes to recognize that an attack is taking place and react appropriately by calling in for police response. However, the patrolling guards in the models have randomized patrol routes, and in this scenario the route occasionally means the guard is close enough to be targeted by Elite attackers. In running this scenario, the guard is damaged (i.e., "injured") 26 percent of the time and destroyed (i.e., "killed) 43 percent of the time.

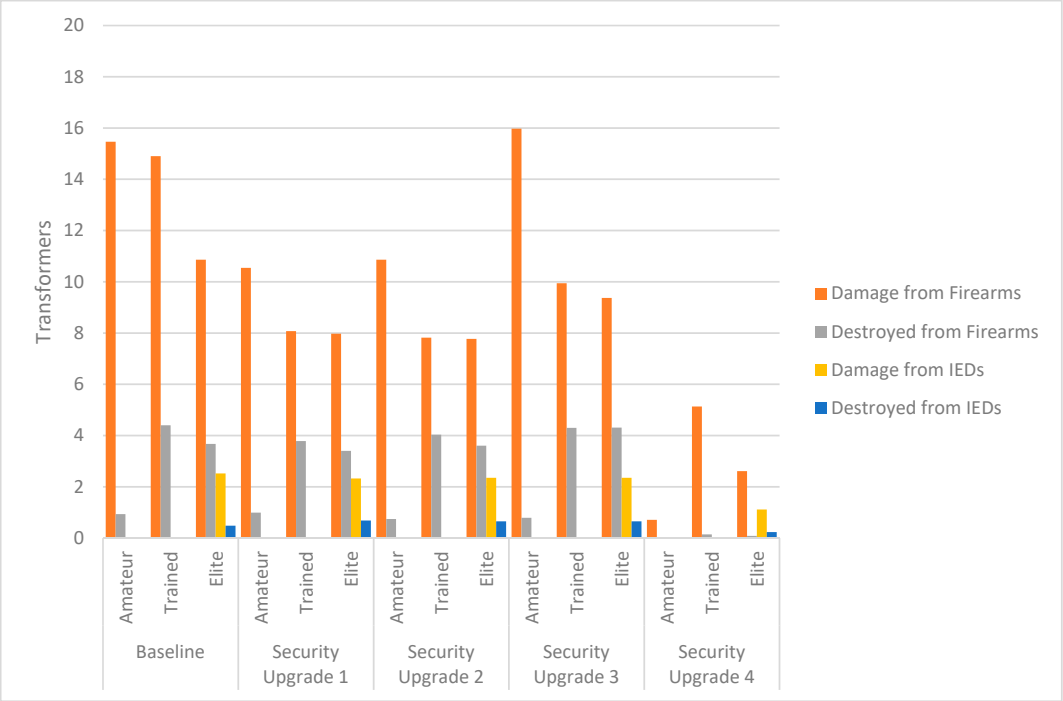

Figure 2. Damaged or Destroyed Transformers from a physical attack, based on Security Upgrade Level.

In Security Upgrade 3, reduction in foliage, increase in lighting, and increase in the number and technological advancement of the cameras and sensors continue to improve. Additionally, a concrete barrier is constructed around the perimeter of the site, in addition to the exterior chain fencing and interior chain fencing. With these security improvements, simulation showed that if the terrain were perfectly flat, each group of attackers would be unable to acquire the targets and all future attacks would be thwarted. Given this development, further interviews were conducted with the military experts at LLNL. They advised that it would be very unlikely that the terrain would be devoid of trees, hills, boulders, or the ability to bring in a vehicle or other device to stand on for greater visibility range. The experts agreed that a flat terrain would not deter attackers and the mission would still be carried out across the various attacker skill levels (Lawrence Livermore National Laboratory, Global Security Program, personal communication, 30 January–1 February 2018). Therefore, a 1.5-m hill was added to the simulations for the Security Upgrade 3 and 4 scenarios. As such, all three attackers improve in the total number of transformers damaged and destroyed on average. As in Security Upgrade 2, an unfortunate patrol route for the security guard results in engagement between the Elite attacker and the guard. The guard is injured 37 percent of the time and killed 40 percent of the time.

In Security Upgrade 4, the most extensive security improvements are implemented. In addition to the incremental foliage reduction, lighting increase, and camera and sensor numbers increasing and technology improvements, gunshot detection sensors and armored shielding around each transformer are added. The shielding reduces the line of sight for the attackers, meaning that acquiring the targets is more difficult. For the Elite attackers, the assailant breaching the perimeter is able to climb the concrete barrier but not get around the armored shielding. The IEDs placed at the bases of the transformers only damage 1.1 transformers on average, and destroys one in less than a quarter of the simulated attacks.

The improvements in technology, such as the gunshot detection sensors, improve the attack recognition and guard reaction time, leading to a quicker police response. As such, the Elite attackers are thwarted, with both the patrolling security guard and responding police arriving to the scene while the attack is still occurring. Because both Elite attackers are within range of responding officers, rather than just one, interpreting the results of injuries and death is slightly different for this scenario. On average, 0.13 out of the two Elite attackers are injured during each of the 100 runs, meaning 6.5 percent of the attackers are injured. Conversely, 1.18 Elite attackers are killed on average during the attack scenario, meaning that in over a total of 100 runs, 59 percent of the time the attackers are killed.

3.2. Cyber-Enabled Physical Attacks

The modeled attack scenarios are all physical attacks. Data on suspected and confirmed attacks show that physical attacks remain a continuous threat against electricity infrastructure, however, the data also indicate that cyberattacks are a rising threat [2]. There has been a rise in lone wolf attacks across critical infrastructure, and cyberattacks may be particularly appealing in that little or no group organization is required to carry out an attack [28]. Furthermore, cyberattacks may offer a sense of security and decreased personal risk, since the orchestrator can conduct the attack remotely.

To assess cyberattack risks, two additional attack scenarios are implemented, each being a cyber-enabled physical attack. A cyber-enabled physical attack is a physical attack in which security features at a site are tampered with remotely (a cyberattack) to assist the onsite attack. In these two attack scenarios, the highest level of security in the model, Security Upgrade Level 4, is attacked first through cyber methods and then by the Trained and the Elite attackers. Prior to the physical attack, the communication lines, security cameras, motion and gunshot detection sensors, and lighting are all disabled through cyber means. It is assumed that Trained and Elite assailants have basic thermal night vision goggles. The physical attacks commence as in the previous scenarios, with the Trained attackers firing from the field and the Elite attackers both firing and breaching the perimeter to place IEDs. Cut communication lines, coupled with the inability to quickly detect the direction of the attack, result in security taking up to one minute to recognize an attack is taking place (a patrolling vehicle guard helps keep this time low) and an additional one-minute delay to react to the attack (the delay stemming from the need to bypass normal radio communications and use cellphones to report an attack instead). Responding police officers take the expected 10 min to arrive on site.

The results of these cyber-enabled physical attacks, as shown in Table 5 and displayed in Figure 3, indicate that the most advanced security improvements continue to help mitigate the damage that could be inflicted from an attack. While, on average, 5.8 transformers are damaged during the Trained attack, fewer than one transformer is destroyed. In the Elite cyber-enabled physical attack, only 1.8 transformers are damaged from firearms and 1.5 damaged from the IEDs, on average. Fewer than one transformer on average is destroyed via either method of attack. Additionally, despite the communication lines being down, which increases the time it takes to call for emergency response, the time it takes the Elite attacker to cut through and climb over the barriers to get into the substation is still enough to result in an encounter with responding police officers. As such, out of 100 runs with two Elite attackers, the attackers are injured 6 percent of the time and killed 93 percent of the time, on average. Figure 4 shows an interaction between security and the Elite Attackers during the cyber-enabled attack in the JCATS simulation.

Table 5. Security Upgrade 4: Cyber-Enabled Attack.

Security Upgrade 4: Cyber-Enabled Attack		Target	Damage from Firearms	Destroyed from Firearms	Damage from IEDs	Destroyed from IEDs
	Trained	Transformer	5.81	0.21	-	-
	Elite	Transformer	1.81	0.07	1.47	0.42
		Elite Attackers	0.12	1.86	0	0
		Security Guard	0	0	0	0
		Police	0	0	0	0

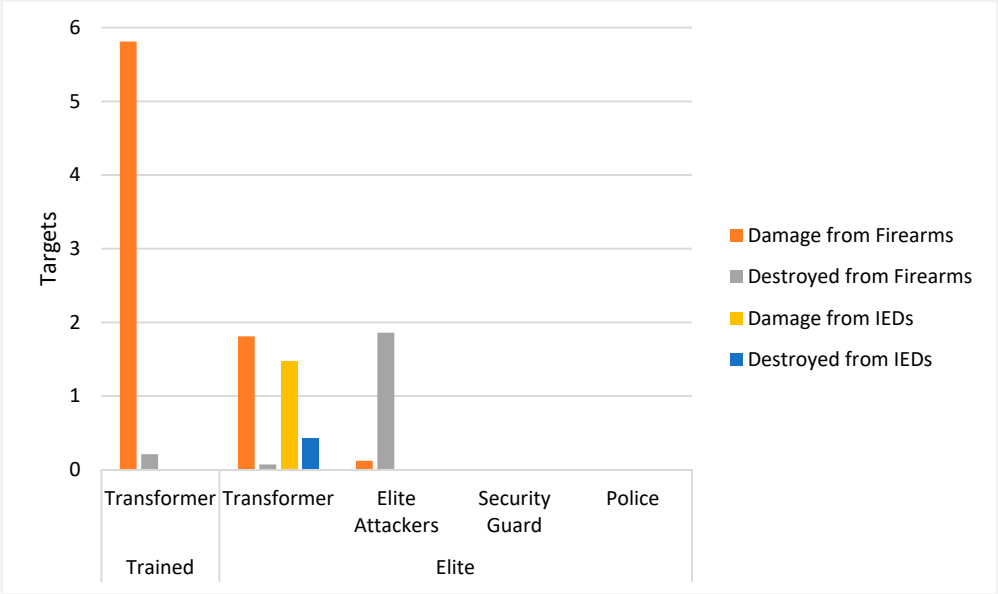

Figure 3. Damaged or Destroyed Targets in Cyber-Enabled Physical Attacks.

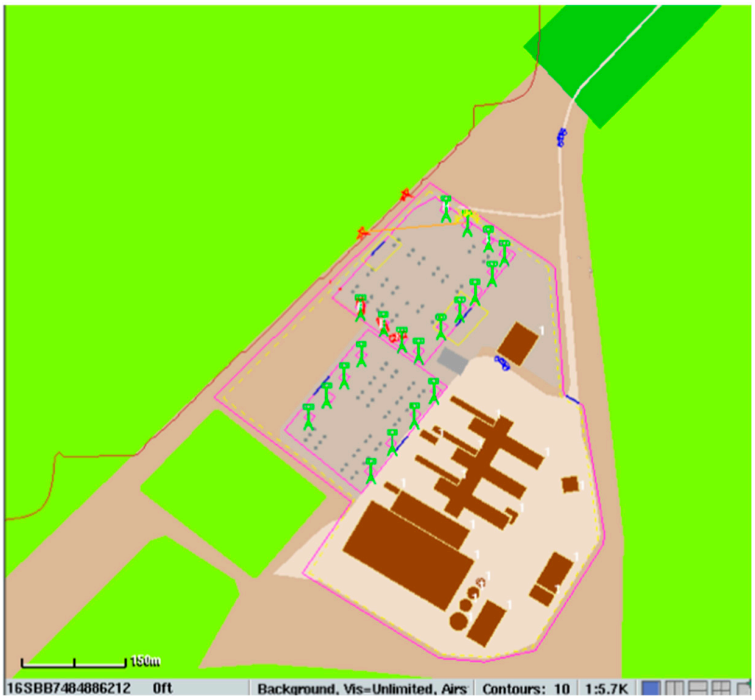

Figure 4. Elite Attackers (red) in a Cyber-Enabled Physical Attack, LLNL-PRES-746039.

4. Discussion

The results of these simulations indicate that for a general substation, such as the one described here, incremental security improvements can mitigate the effects of a physical attack. However, the level of mitigation depends on the security improvement, as some improvements are more effective than others. While clearing vegetation and increasing the amount of light at a site can help the guards detect an attack quickly and reduce hiding places for would-be attackers, the improved visibility also helps attackers have an improved line of site and a higher probability of acquiring the targets. Security cameras have limited effect in thwarting physical attacks, as assailants with firearms can remain outside the range of detection of the cameras and still acquire the targets inside. An increase in the amount of motion sensors woven into or placed on the fencing and external barriers can help make up for this, by detecting shots and the direction of attack earlier. Patrolling guards reduce the response time to confront the attackers, thus potentially ending the attack before the maximum amount of damage can be inflicted on the equipment.

Clearing vegetation, increasing lighting, additional security cameras, and patrolling guards at infrastructure sites are all helpful as well, although a motivated individual, trained to use a firearm, can still implement a fairly damaging attack from outside the security camera's view or a guard's patrol route. Thus, the most effective security improvements come in the form of physical barriers. Table 6 presents a schematic indicating the most effective security upgrade measures that utility owners and regulatory agencies have proposed to implement. Fencing and walls around the perimeter of the sites and internally around key infrastructure, such as transformers, helps reduce the line of sight for would be attackers, though this varies depending on an attacker's ability to secure a better vantage point, such as a naturally occurring higher elevation (a few meters) or bringing in outside structures on which to position themselves. As demonstrated in the security upgrade levels, armored shielding appears to be the preventative measure best equipped to reduce an attacker's line of sight acquisition of a target from both high and low elevation vantage points. Thus, the results of the incremental security upgrade levels, as seen in Figure 2 and Table 6, show the most effective improvements to a site's security come from the following:

- Improved barriers around the substation, such as additional fencing and concrete walls (comparing the Baseline scenario to Security Upgrade 1 and 2).
- Armored shielding around the transformers themselves (comparing Security Upgrade 3 to 4).
- The highest level of security improvements (Security Upgrade 4) can reduce damaged transformers to approximately just 3.5%, 26%, and 18.5% of the total transformers on site, during an Amateur, Trained, and Elite attack, respectively.

Between the Baseline and Security Upgrades 1 and 2, the most substantial security improvement is the implementation of interior chain fencing and improved security cameras and sensors. Given that improvements to vegetation and lighting provide advantages to both defender and perpetrators, and the unlikelihood that security cameras and sensors will be triggered from a firearm attack occurring up to 500 m away, the additional fencing is the only security feature that mitigates damage from the attackers. There are nearly five, seven, and three fewer transformers damaged or destroyed by Amateur, Trained, and Elite attacker's firearm attacks, respectively when additional fencing barriers are added to the sites. Similarly, when terrain is not perfectly flat, a feature added in Security Upgrade 3 that exposes the transformers significantly, armored shielding, results in the most significant drop in damaged and destroyed transformers. Between the Security Upgrade 3 and 4 scenarios, which control for the change in elevation built into the models, there are nearly 16, 11, and 12 fewer transformers damaged or destroyed by Amateur, Trained, and Elite attacker's firearm attacks, respectively.

A notable takeaway from both the initial physical attack scenarios and the cyber-enabled physical attack scenarios is that IEDs are not a very effective method of attack. Firearms, especially coordinated firearm attacks, inflict the most damage on transformers. While aerial drone technology is becoming easier to access, delivering IEDs via drones would likely still be less effective than a firearm attack due

to drone weight limitations. Even if the trained or elite attackers had access to high-end heavy-payload drones that can carry up to 20 pounds [29], military experiments conclude that a solider can carry approximately 75 pounds of additional weight (Lawrence Livermore National Laboratory, Global Security Program, personal communication, 30 January–1 February 2018). Generic IEDs typically weigh between 10–15 pounds (Lawrence Livermore National Laboratory, Global Security Program, personal communication, 30 January–1 February 2018), meaning a single attacker could carry approximately five to seven IEDs while a drone could carry only one to two IEDs.

Table 6. This schematic indicates the effectiveness of security mitigation strategies, where *** indicates the most effective security upgrade measures, ** the second most, and * the third most.

	Baseline	**Security Upgrade 1**	**Security Upgrade 2**	**Security Upgrade 3**	**Security Upgrade 4**
Time of day 	Twilight	Twilight	Twilight	Twilight	Twilight
Lighting 	Deep Twilight	Twilight	Twilight	High (Heavy Overcast)	Extra High (Overcast Sunlight)
Vegetation 	High	Medium	Medium	Low	Low
Perimeter Details 	Chain fence	Chain fence + interior chain fence *	Chain fence + interior chain fence *	Concrete wall + internal chain fence **	... + armored shielding around transformers ***
Cameras/Motion Sensors 	Basic (70% probability of detecting intruder)	Additional Cameras/Sensors (80% probability of detection)	Additional Cameras/Sensors (80% probability of detection)	Advanced cameras + motion sensors weaved into fencing *	SU3 features + gunshot detection sensors **
Security Presence/Engagement 	Two. No patrol, no engagement	Two. No patrol, no engagement	Two, with one patrolling on foot. No engagement *	Two, with one patrolling on foot. No engagement *	Two, with one patrolling in a vehicle. Engagement **

While the preventive measures being proposed by utility companies and NERC are overall useful in mitigating damage from attacks (both outside and inside the perimeter of the substation), the results of this model analysis conclude that security mitigation strategies are most effective when focused on improving physical barriers. Physical barriers, such as additional perimeter and interior fencing, concrete barrier perimeter walls, and especially, armored shielding around the transformers, are the strategies that lead to the greatest reduction in damages from the simulated attacks, as compared across the Security Level Upgrades. Given that IEDs are not as effective as firearm attacks, the results of these simulations indicate that utility owners, operators, and regulatory agencies such as NERC should prioritize how to reduce the vulnerability of substations from firearm attacks.

Ongoing Cyber Threats

This simulation analysis also tested the threats of a cyber-enabled physical attack from both Trained and Elite attackers at Security Upgrade 4, the highest level of security improvements analyzed here. As indicated in the results previously, the most advanced security upgrades proposed by utility operators and regulatory agencies in response to potential cyber-enabled attacks, will not completely eliminate the threats. The main aspect of a cyber-enabled physical attack that allows attackers to damage or destroy transformers is directly related to the increased amount of time it takes to detect and respond to this type of attack. A cyberattack that disrupts communication amongst the operators and security guards within the site, as well as communication to outside emergency responders, will allow attackers to have an even longer timeframe to carry out an attack.

This last concern raises a few points for future security considerations specific to cyber-enabled physical attacks and cyberattacks. Disruption to physical communication and detection equipment (such as phone lines and cameras) are just one component of grid infrastructure that can be impacted during a cyberattack. Denial of service attacks, a method of flooding the computer network with false traffic in order to disrupt normal operations, is an ongoing cyber threat for electricity infrastructure [8]. Furthermore, disruption to the system control data acquisition (SCADA) processes can lead to breakdowns in automated network communications and information being incorrectly interpreted by operators regarding the functionality of the infrastructure [30]. This can result in false trips of breakers and other components of the grid infrastructure, which in turn can lead to confusion amongst operators (if it is unclear where and why the trips are occurring) and result in load loss [30,31]. The cascading blackouts from the 2003 Northeast Blackout demonstrated the magnitude of disruption that false trips can lead to [30]. A cyberattack that focuses on disrupting internal network communications and sending false trip commands can impact an operator's ability to detect and relay unusual activity, ultimately leading to load loss [31].

The threats associated with cyber-enabled physical attacks and cyberattacks to grid infrastructure are vast and constantly evolving. Although grid operators and regulatory agencies such as NERC are indeed focusing on allocating more funding to improve security measures, the possibilities of attack methods are vast. However, with improved grid technologies, such as smart grids, security measures focusing on improving automated disturbance detection and self-healing methods can help mitigate the potential damages from these cyber threats [8].

5. Conclusions

JCATS is used primarily to offer feasible predictions of future attack, wargame simulations, emergency scenarios, or to validate outcomes of past attacks. In this model, the 2013 Metcalf attack is used as a baseline and the model scenarios are validated in that amateur attacks are less successful at damaging or destroying transformers than the actual Metcalf attackers, whereas trained attackers are more successful. However, for the sake of consistency, the model presented in this research kept many parameters consistent across attacker profiles, such as weapon type. It is plausible that the more skilled attackers may choose a different weapon type, thus impacting the ammunition capacity, weapon's range, and target accuracy capabilities. Variations such as this would likely alter the specific numbers of damaged or destroyed targets in some results, but not the overarching findings indicating that the more skilled an attacker is, the more damage they can inflict upon a target. Additional variations to the model to be considered in future iterations of attack scenarios include alterations to attacker behavior. For example, the Elite attacker's behavior could be programed instead for both perpetrators to fire their weapons at the transformers, rather than one perpetrator breaching the perimeter to place IEDs. This would likely be result in a higher damager and destroyed rate of targets, since IEDs do not cause widespread damage to transformers in this model.

The case study demonstrates an approach to evaluating infrastructure vulnerabilities and the efficacy of physical protection methods. The scenarios include plausible attack scenarios based on real attacks, and address vulnerabilities to more sophisticated and coordinated attacks (particularly cyber-enabled attacks). While mitigation strategies proposed by private utilities and encouraged by NERC have the potential to greatly improve physical security standards across the nation's most critical and vulnerable electricity infrastructure sites, the results of this analysis demonstrate the importance of prioritizing the implementation of effective security improvements; namely, physical barriers. Concrete perimeter barriers around the perimeter of sites, along the interior, and armored shielding around technical components such as transformers appear to be the most effective measures to prevent damage from a firearm attack.

The simulation is by no means complete: Even for electrical substations, there may be other attack scenarios and system vulnerabilities not captured here. Future analysis could consider the feasibility and damage estimates from a multi-drone attack. This type of simulation has potential to be

extended to different infrastructure components of the electric grid and other critical infrastructure sectors. Additionally, different kinds of attacks, methods, and assailant capabilities can be expanded into simulations. In particular, cyber-enabled physical and cyberattacks continue to be a growing and evolving risk. Vulnerabilities within the infrastructure software and network configurations present further opportunities for risk mitigation strategies and analysis.

This analysis provides one basis, a starting point, for selecting among choices for physical protection upgrades, and for providing interim estimates of efficacy. Further work is encouraged to link this type of model to cost benefit analysis or other decision frameworks for policymakers and industry officials. While utility sector experts may have advanced modeling and testing capability, the more general scenario developed through JCATS at Lawrence Livermore National Laboratory in this case study provides a basis for policymakers and other decision-makers to evaluate infrastructure vulnerability and attack countermeasures.

Funding: This research was undertaken in collaboration with Lawrence Livermore National Laboratory, but the author received no funding from the Laboratory. This document has gone through the Laboratory-required IM process (reference number LLNL-JRNL-761758-DRAFT).

Acknowledgments: Thank you to Nicholas Matyas with the Conflict Simulation Laboratory (CSL) at Lawrence Livermore National Laboratory for hosting me, assisting in constructing the model, and displaying the simulations. Additional thanks to Mark Piscotty, Hal Brand, Richard Grochowski, Brian Stevenson, and Joe Wilson for their insights and expertise that was integrated into the scenarios. Lastly, thank you to Jovana Helms and Nathaniel Gleason, of the Global Security E-Program at Lawrence Livermore National Laboratory, for making the arrangements for this research to be conducted at the lab.

Conflicts of Interest: The author declares no conflict of interest.

References

1. National Research Council of the National Academies. *Terrorism and the Electric Power Delivery System: Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack*; National Research Council of the National Academies: Washington, DC, USA, 2012.
2. Office of Electricity Delivery & Energy Reliability. Electric Disturbance Events (OE-417). Department of Energy. 2018. Available online: http://www.oe.netl.doe.gov/oe417.aspx (accessed on 1 July 2018).
3. McGrath, J.K. *Targeted Attacks against United States Electricity Infrastructure*; Georgia Institute of Technology: Atlanta, GA, USA, 2018.
4. Smith, R. Assault on California Power Station Raises Alarm on Potential for Terrorism. *Wall Street J.* **2014**, 1–7.
5. North American Electricity Reliability Corporation. *CIP-014-2 Physical Security*; North American Electricity Reliability Corporation: Atlanta, GA, USA, 2015.
6. Lawrence Livermore National Laboratory. *Joint Conflict and Tactical Simulation (JCATS)*; Lawrence Livermore National Laboratory: Livermore, CA, USA, 2017.
7. American Association for the Advancement of Science (AAAS). *Historical Trends in Federal R&D*; AAAS: Washington, DC, USA, 2018.
8. Boroojeni, K.G.; Amini, M.H.; Iyengar, S.S. *Smart Grids: Security and Privacy Issues*, 1st ed.; Springer: Cham, Switzerland, 2016.
9. Mathias, J.-D.; Clark, S.; Onat, N.; Seager, T. An Integrated Dynamical Modeling Perspective for Infrastructure Resilience. *Infrastructures* **2018**, *3*, 11. [CrossRef]
10. Cutter, S.L.; Burton, C.G.; Emrich, C.T. Disaster Resilience Indicators for Benchmarking Baseline Conditions. *J. Homel. Secur. Emerg. Manag.* **2010**, *7*, 1–25. [CrossRef]
11. Liu, W.; Dugar, S.; McCallum, I.; Thapa, G.; See, L.; Khadka, P.; Budhathoki, N.; Brown, S.; Mechler, R.; Fritz, S.; et al. Integrated Participatory and Collaborative Risk Mapping for Enhancing Disaster Resilience. *ISPRS Int. J. Geo-Inf.* **2018**, *7*, 68. [CrossRef]
12. Bahrami, S.; Wong, V.W.S. Security-Constrained Unit Commitment for AC-DC Grids with Generation and Load Uncertainty. *IEEE Trans. Power Syst.* **2018**, *33*, 2717–2732. [CrossRef]
13. Smith, R. U.S. Risks National Blackout from Small-Scale Attack. *Wall Street. J.* **2014**, 1–5.

14. Office of Electricity Delivery & Energy Reliability. *Large Power Transformers and the U.S. Electric Grid*; Office of Electricity Delivery & Energy Reliability: Washington, DC, USA, 2012.
15. California Public Utilities Commission. *Enclosure 5—PG & E Data Response 2, Supplement*; Pacific Gas and Electric Corporation: San Francisco, CA, USA, 2015.
16. Pacific Gas and Electric. PG & E Announces Reward for Information on Metcalf Substation Attack. In *PG&E News Releases*; Pacific Gas and Electric: San Francisco, CA, USA, 2014; p. 1.
17. North American Electricity Reliability Corporation. *State of Reliability 2016*; North American Electricity Reliability Corporation: Atlanta, GA, USA, 2016.
18. North American Electricity Reliability Corporation. *Statement on Physical Security*; North American Electricity Reliability Corporation: Atlanta, GA, USA, 2014.
19. North American Electricity Reliability Corporation. Physical Security Standard Implementation. In *NERC Physical Security Standard Implementation*; North American Electricity Reliability Corporation: Atlanta, GA, USA, 2015.
20. Conflict Simulation Laboratory. *Joint Conflict and Tactical Simulation (JCATS) Capabilities Brief*; Conflict Simulation Laboratory: Livermore, CA, USA, 2018.
21. Conflict Simulation Laboratory. *Conflict Simulation Laboratory*; Conflict Simulation Laboratory: Livermore, CA, USA, 2018.
22. Kincaid, J.P.; Donovan, J.; Pettitt, B. Simulation techniques for training emergency response. *Int. J. Emerg. Manag.* **2003**, *1*, 238. [CrossRef]
23. Bowers, A.; Prochnow, D.L. Multi-Resolution Modeling in the JTLS-JCATS Federation. In Proceedings of the Fall 2003 Simulation Interoperability Workshop, Orlando, FL, USA, 14–19 September 2003; pp. 1–11.
24. Paulo, E.P.; Jimenez, R.; Rowden, B.; Causee, C. Simulation Analysis of a System to Defeat Maritime Improvised Explosive Devices (MIED) in a US Port. *J. Def. Model. Simul. Appl. Methodol. Technol.* **2010**, *7*, 115–125. [CrossRef]
25. James, B.D. Puerto Rican Terrorists Also Threaten Reagan Assassination. *Latin Am. Stud.* **1981**, 1–5.
26. Rosen, A. Incendiary Devices Found Hanging on Tyngsborough Power Lines. 31 March 2016. Available online: https://www.bostonglobe.com/metro/2016/03/31/state-feds-investigate-after-suspicious-devices-are-found-near-power-lines-tyngsborough/olwql3b1ZELqcid2w7JCON/story.html (accessed on 20 November 2018).
27. Lewinski, W.J.; Avery, R.; Dysterheft, J.; Dicks, N.D.; Bushey, J. The real risks during deadly police shootouts: Accuracy of the naive shooter. *Int. J. Police Sci. Manag.* **2015**, *17*, 117–127. [CrossRef]
28. Ellis, P.D. Lone Wolf Terrorism and Weapons of Mass Destruction: An Examination of Capabilities and Countermeasures. *Terror. Political Violence* **2014**, *26*, 211–225. [CrossRef]
29. Brouillette, M. Heavy lifting drones fill a niche. *Mech. Eng.* **2017**, *139*, 23.
30. Coates, G.M.; Hopkinson, K.M.; Graham, S.R.; Kurkowski, S.H. A trust system architecture for SCADA network security. *IEEE Trans. Power Deliv.* **2010**, *25*, 158–169. [CrossRef]
31. Zhang, Y.; Wang, L.; Xiang, Y.; Ten, C.W. Power System Reliability Evaluation with SCADA Cybersecurity Considerations. *IEEE Trans. Smart Grid* **2015**, *6*, 1707–1721. [CrossRef]