Dissertation III

A Quantitative Research Study

on

Probability Risk Assessments in Critical Infrastructure and Homeland Security

Alfred Lee

Liberty University

CJUS 989

Isaiah Stansbery, PhD, Committee Chair

Eugene Ray Belmain, PhD, Committee Reader

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Helms School of Government

Liberty University

2021

PROBABILITY RISK ASSESSMENTS IN CRITICAL INFRASTRUCTURE AND HOMELAND SECURITY

by Alfred B. Lee

A Dissertation Presented in Partial Fulfillment
Of the Requirements for the Degree
Doctor of Philosophy

Liberty University, Lynchburg, VA
2021

APPROVED BY:

Isaiah Stansbery, PhD, Committee Chair

Eugene Ray Belmain, PhD, Committee Member

ABSTRACT

This dissertation encompassed quantitative research on probabilistic risk assessment (PRA) elements in homeland security and the impact on critical infrastructure and key resources. There are 16 crucial infrastructure sectors in homeland security that represent assets, system networks, virtual and physical environments, roads and bridges, transportation, and air travel. The design included the Bayes theorem, a process used in PRAs when determining potential or probable events, causes, outcomes, and risks. The goal is to mitigate the effects of domestic terrorism and natural and man-made disasters, respond to events related to critical infrastructure that can impact the United States, and help protect and secure natural gas pipelines and electrical grid systems. This study provides data from current risk assessment trends in PRAs that can be applied and designed in elements of homeland security and the criminal justice system to help protect critical infrastructures. The dissertation will highlight the aspects of the U.S. Department of Homeland Security National Infrastructure Protection Plan (NIPP). In addition, this framework was employed to examine the criminal justice triangle, explore crime problems and emergency preparedness solutions to protect critical infrastructures, and analyze data relevant to risk assessment procedures for each critical infrastructure identified. Finally, the study addressed the drivers and gaps in research related to protecting and securing natural gas pipelines and electrical grid systems.

Keywords: homeland security, critical infrastructure, probabilistic safety assessment (PSA), T-H-O-risks, domino effect, social network analysis (SNA), failure mode effect and criticality analysis (FMECA)

Copyright Page

Dedication

This research dissertation in criminal justice and homeland security is dedicated to my daughter Sarena Lee and son Alfred B. Lee, Jr. I lost my son in April 2011. Both children have inspired me throughout my educational and spiritual journey at Liberty University. In addition, my dissertation is also dedicated to my mother and father, who have been a driving force in my life in achieving excellence in education and life endeavors. Scripture teaches, “All Scripture is given by inspiration of God, and is profitable for doctrine, for reproof, for correction, and for instruction in righteousness, so that the man of God may be perfect, thoroughly furnished unto all good works. (*King James Bible*, 1769/2021, 2 Timothy 3:16-17).

Acknowledgments

In my ten years as a student at Liberty University, it is appropriate to acknowledge God and all the many instructors, professors, and instrumental people who assisted in completing many higher education programs and doctoral programs. In addition, I would like to recognize family and friends who have provided support in the attainment of all degrees earned at Liberty University. In completing the doctoral program in Criminal Justice and Homeland Security, I would like to thank Isaiah Stansbery, PhD, Committee Chair, and Eugene Ray Belmain, PhD, Committee Member, for their professional educational support. In addition, I would like to thank Fred Newell, PhD, Associate Professor, Online Chair, Helms School of Government Administration Chair, for the steadfast support in this research project and in completing the doctoral program. It is also appropriate to thank all the many support staff and student advisors that have been essential in providing professional online student support. Finally, I would like to thank my mentor, C. Porter, who has provided support since the beginning of my college journey. Scripture teaches, “Go ye therefore and teach all the nations, baptizing them in the name of the Father and Son, and the Holy Ghost. Teaching them to observe all things whatsoever, I have commanded you, and I am with you always, even unto the end of the world” (*King James Bible*, 1769/2021, Matthew 28:19-20).

Table of Contents

List of Figures

List of Abbreviations

Latin hypercube methods (LHS
Dynamic Bayesian network (DBN
ACA: Average-case analysis
AIC: Akaike information criterion
ALARP: As low as is reasonably practicable
API: American Petroleum Institute
ATA: Antiterrorism Act of 1990
BCA: Benefit-cost analysis
BIC: Bayesian information criterion
C2M2: Cybersecurity capability maturity model
CCDA: Casing corrosion direct assessment
CFR: Code of Federal Regulations
CI: Critical infrastructure
CIERA: Critical Infrastructure Elements Resilience Assessment
CIKR: Critical infrastructure and key resources
CISA: Cybersecurity and Infrastructure Security Agency
COPS: Community-oriented policing services
CP: Cathodic protection
CPT: Conditional probability table
CRI: Critical risk indicator
CSIS: Canadian Security Intelligence Service
CTI: Cyber threat intelligence
CVE: Countering violent extremism
CW: Conventional warfare
DAG: Directed acyclic graphs
DEA: Drug Enforcement Administration
DES: Dynamic engineering systems
DET: Dynamic event tree
DHS: Department of Homeland Security
DOE: Department of Energy
DPRA/DPSA: Dynamic probabilistic risk and safety assessment
DST: Dempster-Shafer theory
DtS: Deemed to satisfy
E-CAT: Economic Consequences Analysis Tool
EP: Energy performance
EPS: Electric power systems
ERL: Expected risk-to-life
FBI: Federal Bureau of Investigation
FCRA: Fuzzy-based critical risk analysis
FEMA: Federal Emergency Management Agency
FERC: Federal Energy Regulatory Commission
FISA Court: Foreign Intelligence Surveillance Court
FMECA: Failure mode effect and criticality analysis
FSNA: Fuzzy-based social network analysis

FTA: Fault tree analysis
GAO: Government Accountability Office
GIS: Geographical information system
GLM: Generalized linear model
GPD: Gamma Poisson distribution
GRS: Gas regulation station
GTD: Generation transmission distribution
HIFLD: Homeland infrastructure foundation-level data
HLS: Homeland security
HOE: Human and organizational error
HOF: Human and organizational factors
HSEM: Homeland security and emergency management
HSF: Homeland security framework
HUMINT: Human intelligence
HVE: Homegrown violent extremist
ICO: Infrastructure client organization
ICS: Industrial control system
INGAA: Interstate Natural Gas Association of America
IT: Information technology
IWD: Information Warfare Directorate
JTAC: Joint Terrorism Analysis Centre
KKK: Ku Klux Klan
KPI: Key performance indicator
LCA: Life cycle assessment
LRT: Likelihood ratio test
MCS: Monte-Carlo simulation
MES: Marginal expected shortfall
MFT: Moral foundational and theoretical
MIME: Models of intuitive morality and exemplars
MLR: Multiple logistic regression
MUPRA: Multi-unit PRA
NCW: Non-conventional warfare
NFP: Not-for-profit
NGS: National Grid System
NHBT: Null hypothesis Bayesian testing
NHTS: National Household Travel Survey
NIPP: National Infrastructure Protection Plan
NPP: Nuclear power plant
NSC: National Security Council
NSIRA: National Security and Intelligence Review Agency
NTAS: National Terrorism Advisory System
NTS: National Transmission System
OS: Operational security
OSINT: Open-source intelligence
OT: Operational technology
PBA: Probability bounds analysis

PDF: Poisson density function
PDF: Probability density function
PEM: Point estimate methods
PGM: Probabilistic graphical model
PHM: Prognosis and health monitoring
PHMSA: Pipeline and Hazardous Materials Safety Administration
PIPES: Protecting Our Infrastructure of Pipelines and Enhancing Safety Act of 2020
PPD: Presidential Policy Directive
PRA: Probabilistic risk assessment
PRISMA: Preferred reporting items for systematic reviews and meta-analyses
PSF: Performance-shaping factor
PTSD: Post Traumatic Stress Disorder
QCA: Qualitative content analysis
QRA: Quantitative risk assessment
RAM: Rise Above Movement
RAMS: Reliability, availability, maintainability, and safety/security
RCMP: Royal Canadian Mounted Police
RF-RIM: Risk factor-based reliability importance measure
RRS: Relative risk scores
SAIDI: System Average Interruption Duration Index
SARF: Social amplification of risk framework
SAVI: Systematic analysis of vulnerability to intrusion
SDDSM: Scenario-driven dynamic stochastic model
SDG: Sustainable development goal
SDs: System dynamics
SIGINT: Signal Intelligence
SME: Subject matter expert
SNA: Social network analysis
SUPRA: Single-unit PRA
T-H-O-Risk: Technical, human, and organizational risks
TSA: Transportation Security Administration
UML: Unified Modeling Language
YSCT: YAKINDU State Chart Tools

CHAPTER ONE: INTRODUCTION

Overview

This dissertation will encompass a thorough quantitative research study on probabilistic risk assessments (PRAs) in homeland security and critical infrastructure at the local level of government. The goal is to contribute to future research on securing and protecting critical infrastructure and key resources and provide a methodological approach to address domestic terrorism, violent extremism, risks, and vulnerabilities related to critical infrastructure.

Background

In homeland security, to mitigate risk and vulnerabilities in critical infrastructures, risk assessments are performed to help protect and secure facilities, system networks, operational functions, and essential resources from unexpected events that can occur. In conducting PRAs, a good starting point is examining the historical context, the impact on critical infrastructure and key resources in society, homeland security, risk assessments, elements of domestic terrorism, and theoretical perspectives.

U.S. Department of Homeland Security Historical Context

According to Comiskey (2018), following the September 11, 2001, attacks on American soil, the U.S. Department of Homeland Security (DHS) was established and combined 22 agencies. Today, homeland security strategies are directed toward risk assessments and an all-hazard approach to vulnerabilities, threat assessments, and risk analysis to protect critical infrastructures and key resources. In addition, Comiskey noted that other elements of DHS have specific frameworks and strategies for mitigation, “critical thinking, collaboration, cybersecurity, emergency management, intelligence, law and policy, leadership, preparedness, risk management, strategy, and terrorism” (p. 30). This also includes mitigating emerging elements of violent extremism and domestic terrorism, seen today as a direct threat to homeland security and national security.

Comiskey (2018) further conveyed that homeland security features are centered on leadership skills, risk management processes, security protocols, social identity, and terrorism themes. The fundamental goals of homeland security are to protect the Nation from acts of terrorism, protect critical infrastructures, provide national strategies to mitigate risk, recover from man-made and natural disasters, and respond to accidents and incidents, technology challenges, and malicious manufactured threats and hazards (Comiskey, 2018). Homeland security initially evolved from counterterrorism strategies as a means to assess risk and design to provide countermeasures to mitigate elements of international and domestic terrorist threats on U.S. soil (Comiskey, 2018). Therefore, the dissertation will be focused on PRAs in addressing critical infrastructure and elements of domestic terrorism as a direct threat to homeland security and national security.

Tulumello and Falanga (2021) explained that the term “homeland” represents conceptions of the emergence of community and local practices in public safety to protect citizens from emerging threats. In addition, Tulumello and Falanga emphasized it means cooperation, collaborations, and processes designed to address the “multiscalar geographies of the good and evil made of the coexistence of centrifugal (pushing problems away) and centripetal (incorporating any given outside) dimensions” (p. 1). The DHS provides a systematic approach to homeland security and national security that involves agencies, activities, antiterrorism, counterterrorism efforts, controlling borders, protecting critical infrastructure and key resources, secret service, and the Federal Bureau of Investigation (FBI). Today, Tulumello and Falanga noted that dimensions of homeland security constitute a new scale or level of security that is multiscalar, global, and dimensional concepts that have evolved into a new conceptualization of security and the role law enforcement agencies and community has in public safety, public policy and policymaking. The initial idea of homeland security was designed to legitimize U.S. actions against the emerging threat of global terrorism and respond to emerging threats through the U.S. security apparatus to mitigate global threats and terrorism. Tulumello and Falanga further noted that the DHS elements focus on current and future threats and local efforts designed to promote long-term activity related to safety policies and prevention elements in today’s environment.

According to Sedgwick et al. (2019), law enforcement agencies are encouraged to collaborate and share intelligence and equipment, training, and tactics to mitigate risk, vulnerabilities, and threats in the field of homeland security. The increasing cooperation between law enforcement and federal-level agencies is essential for building community trust (Sedgwick et al., 2019). However, there is little evidence to show collaboration between law enforcement among local jurisdictions, mainly because of political and contextual climates and limits placed on agencies on the local level. In homeland security, to successfully mitigate vulnerabilities and threats, law enforcement agencies in local jurisdictions in a geographical area are required to “increase levels of intergovernmental and interagency cooperation, coordination, and collaboration” (Sedgwick et al., 2019, p. 167). According to Sedgwick et al., in the new era of policing, law enforcement agencies must invest in risk assessment activities, and modern technologies and conduct threat assessments. They must also gather and share intelligence on potential threats and vulnerabilities and domestic terrorist groups identified as operating in the local jurisdiction. The Homeland Security Council encourages interagency cooperation and collaborations between the community and police to promote information sharing to engage in domestic terrorism preparedness. Interagency activities and cooperation in law enforcement networks in homeland security so law enforcement and other agencies can discuss trends, threats, and better ways to disseminate information. In large network meetings, a primary goal is to share intelligence and brainstorm different approaches to communicating information to officers in the field and their agencies (Sedgwick et al., 2019). In homeland security, effectively managing critical infrastructures, and infrastructure protection, conduct risk assessments, and assess risks and vulnerabilities at different levels. In PRAs in homeland security, as it relates to risk, security, and securing critical infrastructure, there are conflicting views, which will be discussed in length in the dissertation, such as how to differentiate probability and consequence and the significance of assessing value against specific conditions and threats.

According to Heyerdahl (2021), to protect critical infrastructures in homeland security, the areas to explore are how to distinguish the difference between risk and probability and understanding the “relationship between the threat against a certain value [asset] and the value’s level of vulnerability” (p. 1), as well as how to mitigate differences based on probabilities and how to measure risk and link these aspects to risk management and decision-making. These are also critical factors that will be addressed in the dissertation using various metrics. Heyerdahl believed gaps in research should also examine the role probability has in risk assessment in government.

Critical Infrastructure Historical Context

The National Infrastructure Protection Plan (NIPP) was instituted in the United States under the DHS Presidential Directive 7 and enacted in 2006 to protect critical infrastructure and key resources (CIKR). In 2009, the NIPP was further updated to provide additional guidance and policies to ensure preparedness and resiliency in the Nation’s critical infrastructure. Since 2013, under the DHS, the NIPP has been the main focal point of national security and for coordinating the Nation's response to critical infrastructure and key resources. To ensure there is an approach to identifying CIKR requires establishing national priorities, goals, and requirements for CIKR protection. In the past ten years, the NIPP has evolved to include cyber-security and an additional role in identifying assets and systems with a statutory mission to ensure the Nation's critical infrastructure receives enhanced protection to help build resiliency, redundancy, and prevent acts of terrorism. The dissertation will highlight case studies relevant to defining critical infrastructure, conducting a risk analysis, probability risk assessments, and physical protection measures. To address cyber security issues, the DHS created the Cyber-Security and Infrastructure Agency (CISA) to address vulnerabilities and protect against cyber threats with additional guidance provided to owners and operators of critical infrastructures.

According to Svegrup et al. (2019), critical infrastructures and key resources provide citizens, businesses, and organizations with resources and services for basic human needs and perform specific emergency and social functions in society. These critical infrastructures include hospitals, communication and technology, food chains, police and fire, hospitals, emergency services, transportation systems, electric power grid systems and transmission, and natural gas providers and transmission lines. Svegrup et al. emphasized that risk assessments are essential in the business environment and focus on factors that can lead to disruptions, affect delivery, and severely underestimate infrastructure's adverse effects leading to damage, disorders, and convulsions. They noted that transmission systems that provide electric power and natural gas produce an economic output and contribute to local economies through employment opportunities (Svegrup et al., 2019). There are also adverse consequences associated with disruptions in the high-order society and when operational functions and system networks lack continuity and redundancy to perform during disruptions. For processes that involve risk assessments, decision-making, and vulnerabilities, the failure to prioritize these areas can produce two direct consequences of vulnerability reduction measures. Measures are reliant on how businesses take a comprehensive approach and require “identifying critical components and adding system components to increase robustness and redundancy” (Svegrup et al., 2019, p. 1970).

Svegrup et al. (2019) explained that critical infrastructures and key resources must be available and provide normal functions and emergency services when adverse consequences lead to disruptions or delays in assistance, service, and help. In addition, Svegrup et al. suggested that risk and vulnerability assessments be focused on factors related to negative impacts to allow system managers and operators of critical infrastructures to mitigate challenges and problems encountered and noted in the evaluation. Svegrup et al.’s views are two-fold, referring to decisions made on vulnerabilities that can impact critical infrastructures and have societal consequences. First, vulnerability-based decisions can require integrating and incorporating an input-output model (Svegrup et al., 2019). Furthermore, Svegrup et al. suggested that for those in a leadership role in critical infrastructure, decision-making is an essential part of the process. Leaders must make decisions that minimize risk and negative consequences in the infrastructure’s behavior, minimize societal impacts and, if necessary, require modeling to determine the best approach (Svegrup et al., 2019). Lastly, Svegrup et al. stated that practical decisions would “provide estimations of high precision and metrics that are accepted by the infrastructure owner(s) and societal actors” (p. 1972).

Topping et al. (2021) noted another significant focal point of governments is assessing targeted attacks against critical infrastructures such as electric power grid systems, natural gas pipelines, and water distribution systems in the United States. These are considered significant infrastructures that provide essential resources to citizens and a substantial part of national security. Topping et al. explained that many of these infrastructures comprise a sectorial and cross-sectorial framework and are interdependent, have interconnectivity in system networks and operational functions, and involve third-party suppliers and operators. According to Kampova et al. (2020), a quantitative approach must also include conducting risk assessments of physical protection measures to mitigate vulnerabilities associated with critical infrastructure. Mitigation must also include countermeasures for physical protection and cyber-attacks by implementing “Systematic Analysis of Vulnerability to Intrusion (SAVI)” (Topping et al., 2021, p. 1) with the utilization of cyber-security software tools and in increasing physical measures. These are elements that will be identified in the dissertation.

Domestic Terrorism Historical Context

Neudecker (2021) pointed out that around the mid-2000s in Western nations, terrorist activities grew, and countries became targets of domestic terrorist movements, often linked to international terrorism. An example of terrorist activity and events is the September 11, 2001, attack on U.S. soil, the terrorist attack in London in 2007, the 2004 terrorist attack involving a train bombing in Madrid, and the 2004 bombing in Istanbul. Neudecker further explained the term “terrorism” is notorious for having different definitions and includes elements of violent extremism, domestic terrorist threats, and international terrorism. In conducting a quantitative meta-analysis of terrorism, Neudecker noted violent activities create fear by exploiting citizens through coercion and organized violence. The goal is to achieve political and social objectives. Domestic terrorism includes individuals and groups associated with separatist movements and religious ideologies. It can consist of “liberalism, anarchism, communism, conservatism, fascism, single-issues, organized crime, right-left-wing, eco-terror, ethnic nationalist, and terrorism perpetrated” (Neudecker, 2021, pp. 1–2) by organized groups and state sponsors of terrorism. How terrorism is defined should derive from a valid and reliable source and research, according to Neudecker.

According to Korstanje (2021), terrorism is not a new phenomenon. However, after September 11, 2001, the dynamics of terrorism have dramatically changed in Western democracies that have faced economic and political challenges and overcoming the COVID-19 pandemic and increases in the virus environment. Korstanje explained that “The War on Terror” (p. 45) has impacted, mined, and eroded elements of democracy in parts of the United States and has impacted checks and balances in federal agencies and institutions of faith. In America and other Western societies, domestic terrorism associated with lone-wolf terrorism has also threatened parts of society. Korstanje suggested lone-wolf terrorism involves a process of radicalization and radicalizing new members through a process in which individuals dislocate themselves from their culture, family, and community and redirect rage at an abstract object and members of society and potentially critical infrastructures. Lone-wolf terrorism has been around since colonial rule, and events after 9-11 have created a radical shift in the dynamics of terrorism in industrial and modern societies. Korstanje explained that the radicalization process occurs through risk associated with the internet, propaganda, and participation in extremist activities and groups that support terrorism and radical ideologies and are isolated from interacting with others and function in small groups, often geographically and separated from the community and family. In the radicalization process, members develop an identity crisis and transform to support violent extremism and conduct acts of terror. Future research should be focused on understanding this type of terrorism and investigate how the methodology impacts today's discipline (Korstanje, 2021).

Sinnar (2019) asserted there are comparative differences in domestic and international terrorism defined in society according to law. Domestic terrorism is violence committed for purely domestic political reasons and "its origins and intended impact" (Sinnar, 2019, p. 1333). For Sinnar, there is a divide between domestic and international terrorism laws. The rationale behind each form of terrorism is based on three factors related to the impact terrorism has on civil liberties, views of federalism, consequences associated with the magnitude of the threat and effects of a terrorist attack, and how acts of violence are perpetrated and performed. Sinnar also explained that under U.S. law, and when there are acts of terrorism committed, a decision is made on whether it is domestic terrorism in nature or linked to international terrorism. An assessment of acts of domestic terrorism is reliant on evaluations conducted by the FBI and based on the investigation, the police report, and prosecution, determining if an act of terrorism is linked to a specific cause, ideology, political agenda, and community (Sinnar, 2019). In any case, involving domestic or international terrorism, the FBI is the lead investigative agency. Sinnar further suggested that critics believe terrorist behavior is associated with "race, religion, or the ideological perspective of terrorists and whether government officials and the media conceptualized such acts as terrorism" (Sinnar, 2019, p. 1335). Additionally, in cases when an individual(s) suspected of having links to terrorism, and has phone conversations concerning potential acts of terrorism, uses the internet to radicalize new members, provides material support, and conspires with known terrorists, under the Foreign Intelligence Surveillance Court (FISA Court), law enforcement officials will obtain a search warrant in an attempt to "intercept conversations and to obtain internet records" (Sinnar, 2019, p. 1335).

In examining cases of terrorism in the United States, Tschantret (2020) noted that the goal is to conduct a multilevel statistical analysis of events involving domestic terrorism in America dating back between 1970 and 2015. For example, the 1995 Oklahoma City bombing involving the Alfred P. Murrah Federal Building and the 2016 Pulse Nightclub shooting in Orlando, Florida, demonstrate how lethal domestic terrorist attacks can target critical infrastructures and events (Tschantret, 2020). Furthermore, in 2020, another example of a domestic terrorist attack took place in the U.S. capital, one of the most prominent government infrastructures in Washington, DC (Tschantret, 2020). Therefore, to mitigate future extremist acts of violence and terrorism, research involving domestic terrorists should be focused on the ability to protect and secure critical infrastructures and focus on the "variation in terrorist attack lethality" (Tschantret, 2020, p. 235). These factors are crucial in understanding the capabilities of specific designated domestic terrorist groups, organizations, and lone-wolf actors.

Critical infrastructures are often not seen, in the present tense or in plain view of the general public in parts of society, such as electric power grids and electrical lines and natural gas pipelines, water filtration systems, dams, and community hospitals. Protecting these infrastructures requires government, leaders, owners, and operators to conduct timely risk assessments. The overall goal is to protect against cyber-criminals and provide physical protection to protect these facilities. Therefore, estimates should include measuring the probability of a potential terrorist attack, disruption, and damage to the Nation's most critical infrastructures.

Critical Infrastructures and Key Resources in Society

According to Rehak et al. (2019), to manage critical infrastructure and key resources effectively, owners and operators must conduct PRAs and assess facilities and resources for resiliency to determine the reliability of service, resources, and commodities to minimize societal impact. Rehak et al. suggested resilience and resiliency are critical factors that help reduce risk and vulnerabilities and help absorb the impact of damage, disruption, and system failures caused by accidents, disasters, and deliberate factors. To assess critical infrastructures, the Critical Infrastructure Elements Resilience Assessment (CIERA) is a tool used to perform a statistical assessment and analysis of the level of resiliency in elements of infrastructures to help determine if infrastructures can recover from a disaster or disruption (Rehak et al., 2019). The process involves a thorough evaluation of critical infrastructure sectors such as electrical grids, communication networks, and natural gas transmission lines. In addition, Rehak et al. also suggested the CIERA program offer owner and operators the ability to perform analysis and assessment of essential functions. Resiliency ensures that infrastructures and resources have the "ability to anticipate, absorb, adapt to, and or rapidly recover from a potentially disruptive event" (Rehak et al., 2019, p. 4).

Dick et al. (2019) found that resilience and resiliency are integral to modern society in one case study. Learning concepts promoting deep learning in the homeland security field can involve applying machine intelligence and computer technology and system applications design to develop learning patterns and produce data and image analysis on specific interest categories and particular infrastructures. According to Dick et al., deep learning can contribute to 95% accuracy and reduce problems in power-related infrastructures such as electrical grid systems when elements of deep learning and machine vision are applied to protect critical infrastructures. Deep learning is a concept that involves machine vision and computer system imagery to assess factors related to risk and threat assessments and operational functions by evaluating learning patterns to produce exemplar data to use as part of preventive maintenance (Dick et al., 2019). In society, critical infrastructures such as processing facilities and system networks, health safety networks, and institutions essential to security and economic well-being, high-technology innovations can detect anomalies before failures occur in processes (Dick et al., 2019). Scripture teaches, “These were noble men than those in Thessalonica, in that they received the word with all readiness of mind, and search the Scripture daily, to whether those things were so” (*King James Bible*, 1769/2021 Acts 17:11).

According to Pirbhulal et al. (2021), protecting system networks and operational functions requires an analysis of reliability, availability, maintainability, and safety/security (RAMS). Furthermore, an investigative process ensures that critical infrastructure and resources are protected against vulnerabilities. The goal is to prevent failures in modes in system applications. Therefore, it is a view that cyber-security tools are needed to safeguard digitization in digital components in system networks, which is essential in protecting critical infrastructure systems and operational processes (Pirbhulal et al., 2021).

Dawson et al. (2021) suggested that managing critical infrastructure cybersecurity is a significant challenge because of vulnerabilities and risks that can impact the 16 crucial infrastructures from a national and global perspective, and they noted the purpose of the Presidential Policy Directive (PPD) 21 on Critical Infrastructure Security and Resilience is to help mitigate cybersecurity attacks. The PPD 21 is designed to provide enhanced protection for infrastructure sectors that include policy and mitigations to “strengthen and maintain secure, functioning and resilient critical infrastructure,” according to Dawson et al. (2021, p. 69). Challenges and problems facing critical infrastructures on the national and global level are associated with cyber warfare, ransomware, and denial of service attacks driven by cyber-criminals. These problems can have a large-scale and cascading impact on system networks and the operational functions of significant infrastructures because cyber-criminals design ransomware to take control of system networks for ransom. Therefore, mitigation is an essential part of addressing the problems caused by these cyber-criminals.

According to Luskova and Dvorak (2019), in managing risk, leaders and management staff must understand critical infrastructures are considered an asset or system, and any type of disruption, damage, or cyber-attack can have an adverse impact on the ability to perform as intended and can have an impact on the performance of the economic and financial sectors, and the ability provide for the needs of citizens and services relative to the quality of life (Luskova and Dvorak, 2019, p. 7). In addition, because of new technological advancements in society, leaders must prepare for unforeseen problems that require enhancing security protection measures and an increased level of security to protect facilities, property, people, the environment, system networks, and critical infrastructure. In homeland security and the private sector, risk management is a core feature, and leaders must be prepared to evaluate exposure to certain risk factors that can impact the energy sector, information and communication technologies, roads and bridges, and the ability of first responders to respond effectively, according to Luskova and Dvorak. In risk management, leaders follow predetermined guidelines and management processes to mitigate current challenges and future problems that can occur.

Homeland Security in Society

In society today, homeland security aspects have evolved to focus more on domestic terrorism, cyber-security, preventive measures, interdiction, enhancing counterintelligence and counterterrorism measures, data-driven intelligence, and information sharing, vaccinations and preventing the further spread of COVID-19, and other concepts essential in mitigating threats and protecting critical infrastructures and key resources (Bellavita, 2019). The learning concepts on aspects of homeland security involve three factors: (a) foundational concepts on elements of homeland security, (b) images that validate homeland security concepts, and (c) concepts that subjectively include ideas that offer research questions and foundations and provide helpful knowledge in the homeland security field (Bellavita, 2019). In addition, Bellavita noted that empirical knowledge will help link physical and material sciences elements that include safety, security, physical aspects of homeland security, biological factors related to the environment, chemistry and chemical hazards, engineering, and information systems and technology.

Haase and Demiroz (2020) stated that communities are better prepared when they engage in activities to reduce risks and increase resilience and resiliency to respond to dangers, vulnerabilities, domestic threats, disasters, and disruptive events in homeland security. They believe the best way to help communities understand the benefits of resiliency "in the community is to enable the concept to be applied in research and public policy contexts" (Haase & Demiroz, 2020, p. 1). Additionally, Haase and Demiroz mentioned that *Homeland Security Affairs* and the *Journal of Homeland Security and Emergency Management* are resources that provide literature on resiliency in homeland security to communities and agencies to help develop a hybrid model that conceptualizes elements of resilience and resiliency. It is also essential for society and communities to understand how federal agencies define stability and resiliency at different governmental levels, such as the White House, Department of State, and DHS. Haase and Demiroz further noted that these efforts could impact the design, implementation, programs, management, and evaluation of public programs and policies without a clear understanding of the terms.

Danko (2019) explained that experiential is a common feature in homeland security and emergency management (HSEM) in higher education and a methodological approach that represents a shift in homeland security elements. Addressing the challenges and problems seen in society to protect citizens, government, and critical infrastructures from threats requires supporting a national strategic strategy. After September 11, 2001, terrorist attack on U. S. soil, in 2003, President Bush created the DHS as a national strategy to respond to terrorism, prevent terrorism, border security, cyber-security, respond to hazards, and develop disaster resilience. Since its inception, the mission of the DHS has changed due to risk, vulnerabilities and emerging threats, and increased domestic terrorism. The DHS provides a framework to agencies to help prevent future terrorist attacks and pending threats to safeguard America. Danko further noted that today, higher education programs on homeland security emergency management are structured to provide a transformational and evidence-based learning approach through experience, best practices, and research. Future research should examine the research gaps and students' abilities to obtain robust analysis concerning risk and research design to bridge the gap and provide ways to assess essential skills to achieve student success (Danko, 2019). Examining risk and research gaps can include ensuring students are provided with an environment to improve critical thinking skills, perform a critical analysis involving complex problems and situations, and engage in collaborative problem-solving in an experiential learning environment and practice to address today's challenges and issues (Danko, 2019).

Risk Assessments in Society

According to Deka and Fei (2019), conducting a risk assessment on critical infrastructure and individual users is essential in planning and developing homeland security strategies for transportation systems in society, communities, neighborhoods, and ride-sourcing. Under the guidance of the Bureau of Transportation Statistics and the DHS, in 2018, the National Household Travel Survey (NHTS) was used to develop a statistical dataset to help analyze characteristics of neighborhood transportation systems and ride-sourcing user data from limousine and taxi trip frequencies to provide data on the proximity of transportation systems and ridesharing sources to neighborhoods (Deka & Fei, 2019). In a research study, Deka and Fei found that the frequency of citizens using ridesharing increased, and people living in proximity to transit systems use ridesharing more frequently. Data and other information provided are essential to homeland security in providing homeland infrastructure foundation-level data (HIFLD) to the DHS for empirical statistical modeling to understand the impact ridesharing and other transportation systems have on neighborhoods to assess travel needs (Deka & Fei, 2019). In society, public transportation serves as a safety net for the less privileged and underserved living in rural communities and metropolitan neighborhood areas.

Deka and Fei (2019) suggest that for future research, the DHS and the NHTS should conduct a national study on the implications ridesharing has on transportation systems nationwide through national surveys. It is vital to execute risk assessment in a society that lacks protections for critical infrastructure and key resources. Data and statistics are collected to help policymakers and local government planners to understand probabilities and the need to extend electrical power grid systems and natural gas pipelines or build hospitals, bridges, roads, and emergency services.

Recently, DHS agencies have been under enormous strain and dealing with risks associated with the environment resulting from the COVID-19 pandemic which has been a significant homeland security concern. Citizens and loved ones have been overcome, and many have died from the COVID-19 pandemic. State and federal government agencies and the country have been under enormous challenges and problems, including a time of political turmoil and a change in presidential leadership in the United States. It is a critical time worldwide, and people have relied on their faith in God and prayer to help overcome challenges and problems. Scripture teaches, “But without faith, it is impossible to please him; for he, that cometh to God must believe that he is, and he is a rewarder of them that diligently seek him” (*King James Bible*, 1769/2021, Hebrews 11:6).

Anthony and Hermans (2020) suggested that risk management and resiliency are leadership processes concerned with improving critical functions and systems to support neighborhoods, local areas, groups of people, and critical infrastructure in the homeland security profession. Resiliency and resilience planning in homeland security agencies and organizations allow leaders effectively to respond to and recover from man-made and natural disasters. Resiliency is a process that involves developing the capacity to maintain continuity and bounce back after disruptions, damage, and terrorist attacks to critical infrastructure and key resources. According to Anthony and Hermans, resiliency in spiritual life is encompassed by “both individual and communal perspectives and presupposes self-transcendence as an experience of being drawn beyond by something outside of oneself, being and liberated from one’s fixation on oneself” (p. 66). Furthermore, spiritual and religious discernment is considered a core feature of spiritual life driven by assessing personal spiritual traits relying on spiritual capital and lived spiritual experiences (Anthony & Hermans, 2020). Spiritual life creates resiliency and a higher order of values and levels that followers support the religious organization’s vision and mission (Anthony & Hermans, 2020). Scripture teaches, “Jesus said I am the way, the truth life; no man cometh unto the Father, but by me” (*King James Bible*, 1769/2021, John 14:6).

Winterfeldt et al. (2020) explained that to assess risks involved with domestic terrorism, a risk cost-benefit analysis is a methodological approach used in risk management to examine the benefits, research cost, and total cost from the start-to-start finish. Risk-informed benefit-cost analysis in homeland security is essential. It allows analysts, policymakers, and researchers to estimate future damage caused by domestic or international terrorist attacks and threats, including damage associated with natural or manufactured disasters. Winterfeldt et al. emphasized that the Economic Consequences Analysis Tool (E-CAT) provides policymakers and analysts with the probability of the economic impact of specific threats listed in the Homeland Security National Risk Characterization Register. The homeland security factors related to cost-benefits analysis vary according to the agency and research project, the type of testing, and the sensitive nature of a research project (Winderfeldt et al., 2020). Through this process, lessons are learned for future applications, intelligence products, and tasks to provide a baseline risk metric to make comparisons in research (Winterfeldt et al., 2020). A risk cost-benefits analysis is also essential in analyzing potential damage and destruction caused by an extremist, domestic terrorist, or natural disaster and provides and has a role in PRAs in assessing critical infrastructure and elements of homeland security and managing risk.

According to Suo et al. (2019), in addressing problems related to critical infrastructures in homeland security and the private sector, there are benefits in conducting risk assessment in society, especially to meet the demand for public improvements, services, utilities, and improvements in critical infrastructure. According to Suo et al., risk assessment provides a profile of existing conditions, future risks, and potential sources of risk. A theoretical approach to risk assessment can include a hybrid model. This model focuses on risk characteristics such as a system-of-systems perspective, examining dual interdependency, and a scenario-driven course to examine complexities and explore emergency response planning and can include a four-stage approach resolution framework and risk matrix. These quantitative factors will be discussed and highlighted in data and graphs at each dissertation stage.

According to Kumar et al. (2021), to address gaps in research regarding risk assessments and resilience in critical infrastructure, risk management processes must include a risk profile to consider the impact of climate change to withstand events that can occur in the present and future. Therefore, Kumar et al. explained that research mitigation must include extreme events from a global perspective in a framework design to improve resiliency in critical infrastructures. The dissertation research will provide data and methods to predict climate projections and the probability of the impact on critical infrastructure using probability risk assessments. According to Kumar et al., the PRA approach will allow researchers to examine limits and limitations related to distribution and variables based on specific patterns and vulnerability to climate change.

Yao et al. (2020) suggested an essential part of the process is understanding the probability of an occurrence by conducting a PRA of any limitations, the target, or the targeted area to mitigate concerns. It also includes exploring gaps in research associated with the historical context and collecting data from models used to evaluate the likelihood of an attack or event. Yao et al. noted that models such as the Elkabets and Shohet model and game theory could be applied to explore gaps in research regarding the level of protection needed to protect infrastructure or a problem-defense focus model designed to take into account consideration security at different levels.

In today’s volatile environment and society, Baggott and Santos (2020) asserted that examining protection measures for the Nation’s power grid system and natural gas pipeline network requires investigating vulnerabilities. Therefore, it also includes robust risk analysis in a framework that considers a multitude of problems that can occur to impact operational functions and system networks that control infrastructures and involve other interdependent infrastructures that rely on resources to function. In addition, leaders, owners, and operators must take necessary measures to prevent and mitigate vulnerabilities and probabilities associated with cyber-attacks, hacking, and domestic and international terrorism by formulating strategies, according to Baggott and Santos. To focus on many of these problems, data in the proposed research will highlight “severity and likelihood classifications” (Baggott & Santos, 2020, p. 1754), and evaluate six scenarios in different phases, and cover the spectrum of problems that can occur.

Domestic Terrorism in Society

According to Sacco (2021), domestic terrorism is significantly different from criminal activity and centers on self-motivated individuals driven by a specific cause, ideology, or political agenda. Domestic terrorists are divergent and draw beliefs from different philosophical views and worldviews to justify violent extremism and domestic terrorism directed at the government for political reasons (Sacco, 2021). In addition, Sacco explained that domestic terrorists are ideologically motivated or driven by a specific cause, and acts of domestic terrorism can be considered hate crimes and classified as domestic terrorism when an ideology or an individual fuels acts of violence as a member of a domestic terrorist group. Acts of domestic terrorism include intentionally selecting the “victim’s actual or perceived race, color, religion, national origin, gender, gender identity disability, or sexual orientation” (Sacco, 2021, p. 2). Homegrown extremists are often radicalized and motivated by foreign terrorist groups and organizations that provide material support and support the groups’ ideologies. They may act independently under the direction of the leader of the terrorist organization through propaganda or communication through the internet (Sacco, 2021). There are also underlying drivers of domestic terrorism driven by perceived or “perceptions of government or law enforcement overreach, sociopolitical conditions, racism, anti-Semitism, Islamophobia, misogyny, and reactions to legislative actions” (Sacco, 2021, pp. 2–3). The FBI considers violent domestic extremism as an act of violence fueled by radical and violent extremists.

Kurz (2020) stated understanding elements of terrorism and the dynamics require examining gaps in research on domestic terrorism and international terrorism and recognizing the Code of Federal Regulations (CFR) defines acts of terrorism as the unlawful use of physical force and violence and acts of violence committed against citizens of a populated area and violence that causes severe property damage, to intimidate or coerce a government, and parts of the civilian population. Those who promote terrorism and acts of violence are committed to supporting a political agenda, social objectives, religious and jihadist viewpoints, and radicalization process (Kurz, 2020). A broad definition of domestic terrorism includes acts of violence committed by White supremacists, misguided militias, lone-wolves, and other violent extremists motivated by ideologies, political views, and acts of violence in furtherance of a cause. According to Kurz, domestic terrorism has domestic origins in parts of society within the U. S. territorial jurisdictions. Extremists support ideologies and become radicalized and engage in planning and actions to conduct terrorist attacks within the United States. This type of terrorism is currently the greatest threat to the United States and requires counterterrorism measures to mitigate threats. According to Kurz, since September 11, 2001, at least “seventy-three percent of deaths” (p. 119) have been associated with violent extremism and domestic terrorism. Kurz also noted that most cases involving domestic terrorism fall under the U.S. PATRIOT Act, and international terrorism involves acts of terrorism that occur outside “of the territorial jurisdiction of the United States or transcends national boundaries” (p. 119). International terrorism falls under international and federal terrorism laws, and terrorists are extradited to the United States for criminal prosecution. Scripture teaches, “Fear not for I am with you, be not dismayed for I am your God. I will strengthen you. I will help you. I will uphold you with my righteous right hand" (*King James Bible*, 1769/2021, Isaiah 41:10).

Problem Statement

In examining homeland security and critical infrastructure problems related to domestic terrorism and violent extremism, P. Davis (2019) noted on September 19, 2019, in the United States, a man trained in bomb-making was indicted for conducting surveillance and targeting potential targets for a terrorist organization. This suggests a significant problem related to targeted violence and homegrown terrorists and why local law enforcement officials must remain on guard for the evolving threat environment facing the United States and critical infrastructures (P. Davis, 2019). In addition, after the domestic terrorist attack in El Paso, Texas, that violent extremists perpetrated to support state and local law enforcement partners, the FBI in 2019 established the "F.B.I.'s" "domestic terrorism-hate crimes Fusion cell " (P. Davis, 2019, p. 11). The goal is to provide law enforcement partners with investigative and intelligence support to mitigate the threat of domestic terrorism. P. Davis also noted another purpose is to ensure the seamless sharing of information among local law enforcement agencies and investigative resources concerning the threat environment. According to P. Davis, in a January 2019 press conference, the FBI director stated the domestic-terrorism cases "investigated are motivated by some version of what you might call white-supremacist violence" (p. 12), and it is not the extremist ideology investigated; it is the violence investigated.

Molstad (2020) emphasized another problem in the United States is that there is no uniform framework for specifically prosecuting domestic terrorism, but criminal codes are applied to prosecute specific acts of terrorism. According to Molstad, political interest and protectionism fuel attempts to curb laws involving right-wing terrorism to avoid conviction under terrorism laws and sections of the criminal code. Molstad suggested citizens in society feel the judicial system should incorporate a form of law or a uniform domestic terrorism statute that will allow for a criminal prosecution not based on a belief system, but on the perpetrators' extremist violent actions and intent. For example, the problem here suggests that right-wing and left-wing extremists believe their way of life is infringed upon and that their personal or national way of life is threatened and resort to violent extremist behavior to support political and ideological beliefs and commit acts of violence punishable by law, according to Molstad. Scripture teaches, "For whosoever shall keep the law, and yet offend in one point he is guilty of all" (*King James Bible*, 1769/2021, James 2:10).

Theoretical Perspectives

Homeland Security Theories

According to Comiskey (2018), homeland security is a discipline. It lacks a specific theory or framework, but learning can involve multiple concepts and ideas taught by professionals from various fields related to homeland security. Comiskey explained that institutions and homeland security elements have evolved from numerous disciplines evaluated, validated, developed, and generate other theories and methodologies as the field matures over time. Homeland security is also a discipline in which multiple realities in society became known and can include a different body of knowledge-based, theoretical perspectives, or overarching framework based on the subject matter or homeland security concern (Comiskey, 2018). *Bothamley's Dictionary of Theories* in 2002 referred to homeland security as a general activity and principles that are evidence-based and supported by scientific evidence which explains observed facts and phenomena (Comiskey, 2018). Theoretical perspectives can also include typologies and evidence-based and systematic viewpoints in homeland security. According to

Comiskey, theories in research can involve “descriptive theory and explanatory theory, normative theory, and predictive theory” (p. 31), and the inductive process is referred to as a grounded theory. Other theories include “grand theory, macro-theory meso-theory, and micro theory” (Comiskey, 2018, p. 31). Homeland security is considered a metadiscipline because of the cumulative knowledge, methods used in inquiries, and problem-solving to solve complex and critical problems (Comiskey. 2018).

Stewart and Oliver (2021) noted elements of homeland security engage in policing programs, crime-fighting initiatives, counterterrorism programs, and community-oriented policing services (COPS) programs at the local government level. These programs receive funding allocations through the DHS. At the local level of government, funding initiatives and financial incentives support strategic planning, operational goals, tactical necessity, and change to adapt at the local level (Stewart & Oliver, 2021). The DHS comprises 22 departments and federal agencies responsible for responding to natural or manufactured disasters and terrorist incidents; the agencies involved represent various disciplines and thus approach different challenges and problems from different theoretical perspectives, as noted by Stewart and Oliver. Scripture teaches, “Thus said the Lord the maker thereof, the Lord that formed it, to establish it, the Lord is His name” (*King James Bible*, 1769/2021, Jeremiah 33:2)

Risk Assessments Theoretical Perspectives

From a theoretical perspective, risk assessments in homeland security structured for critical infrastructure are considered concepts, ideas, and processes designed to identify and analyze hazards, vulnerabilities, and threats that can adversely impact system networks, operational functions, and business processes. The data collected allow leaders, policymakers, owners, and operators to make informed decisions and mitigate risks. The theoretical perspective in the dissertation will consist of PRA theories involving electrical power grid systems and natural gas pipelines.

Critical Infrastructures Theories

According to Ren et al. (2020), in a quantitative approach to critical infrastructures, grounded theory is a model used to examine conditions and losses in homeland security and inferences in the relocation of victims' "self-identity, social connections, and meaning systems" (p. 1) during disasters. This approach includes a model designed to assess mental health and provide services and support relocation policy in a postdisaster environment and developed to evaluate conditions that lead to psychological disorders (e.g., posttraumatic stress disorder [PTSD]) and problems due to relocating citizens and victims in heavily damaged areas caused by earthquakes or significant disasters (Ren et al., 2020). The benefit of this model is in assessing victims, the relocation process, psychological and social vulnerabilities, and cultural factors related to disease, mental health, domestic terrorism, and other problems. According to Ren et al., future researchers should consider this model and examine the benefit of mental health services during disasters, support systems, and cultural significance.

Meijer et al. (2021) noted that viewing critical infrastructures such as drinking water facilities, electrical grids, and natural gas transmission lines is essential to the well-being of life and citizens living in communities and cities. In these distribution systems, risk assessments and maintenance strategies are crucial to the efficiency of operations and vital functions. They suggest graph theory used to assess and identify the most critical elements such as water supply and demand and to, categorize sewage discharge systems elements, and measure the distance between manufactured overflow systems and structures to provide a graphic presentation of networks involving water and sewage distribution systems, electrical networks, and grid systems (Meijer et al., 2021).

Grady et al. (2021) noted that Maslow’s theory of human motivation could be used to approach the hierarchical arrangement of critical infrastructure based on societal and basic human needs. This theory addresses needs and social vulnerabilities related to supply availability and demand. This theoretical approach can help guide system networks, and physical critical infrastructure systems failures and political governance theories are applied when evaluating functions related to public welfare and addressing the basic needs of consumers. According to Grady et al., the government’s role in providing for underserved communities and communities “developed under welfare capitalism to coordinate public and private efforts for finance and delivery of social welfare” (p. 10) in critical infrastructure management.

Domestic Terrorism Theories

According to Varaine (2019), in viewing conflicting views on economic deprivation and terrorism, one hypothesis suggests economic deprivation has no relation to terrorism. Still, Varaine argued that economic deprivation and terrorism are related to the extent to which collective deprivation is a factor in determining the role ideology plays in terrorist movements, such as the ability of far-right terrorists to mobilize because of collective deprivation far-left terrorist mobilization is motivated by collaborative improvements. Varaine further noted that system-justification and backlash theories are consistent with how far-left and far-right terrorism mobilizes, and the decline or increase in economic activity serves as potential drivers. Finally, Varaine mentioned that some conservative political systems support right-wing ideologies, and conservative extremists express political attitudes. Collective action and extremism are at the heart of conservatism when motivation levels and similar views are described on the far left (Varaine, 2019).

According to A. P. Davis and Zhang (2019), civil society has had exposure to domestic terrorism. Between 1970 to 2010, there have been 167 domestic terrorist attacks across the country, and terrorist organizations engage in high-risk activities and movements that present a threat to other countries. Thus, social movement theory can help clarify an element of terrorism and explain terrorism rooted in an organizational paradigm (A. P. Davis & Zhang, 2019). Furthermore, social movement theory can also help explain the radicalization process, how domestic terrorist organizations become a radical social movement, and how organizations become spaces for radicalization and challenge political structures, as noted by A. P. Davis and Zhang.

According to Qvortrup (2020), the Lijphart model of domestic terrorism suggests that domestic terrorism is motivated by a grievance that leads to opportunities for meaningful participation. In this model, when there are more opportunities for political influence, domestic terror and fatal acts of terrorism are lower; terrorist groups will not have the ability to perpetrate domestic terror. Additionally, Qvortrup explained domestic terrorism can be associated with factors related to ethnicity and ethnic tensions, linguistic and religious culture, and minority discrimination. Qvortrup provided an opposing view on the “logic of scientific discovery” (p. 908) by Popper. In choosing a specific theory on domestic terrorism or any other subject, Qvortrup suggested a hypothesis or thesis should not be introduced if the theory cannot “explain the things the former theory could explain, as well as the things it could not explain” (p. 908).

According to Haddow et al. (2021) in the United States, domestic terrorist groups and organizations that include the Ku Klux Klan (KKK), militias, and Oath Keepers (identified as white supremacist organizations) engage in lynchings, intimidation, burning crosses, voter intimidation, and action designed to impact and influence the political process. Haddow et al. (2021) suggest anarchists have been around since 1886, engaging in demonstrations, mail bombings, and rallies, and are “responsible for two of the ten deadliest attacks on American soil” (Haddow et al., 2021, p. 410). In addition, unions have been noted to engage in terrorism to influence the political process. Other terrorist groups and organizations identified are groups or organizations with violent and destructive natures and engage in violent activity and behavior. For example, according to Qvortrup, domestic terrorist organizations are identified as the “K.K.K., the Black Panthers, Weather Underground, Army of God, Earth Liberation Front, Animal Liberation Front, Aryan Nations, the Boricua Popular Army, the Jewish Defense League, and the Symbionese Liberation Army” (p. 410). Haddow et al. further suggested one of the single most devasting acts of domestic terrorism in the United States was the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City.

State of Problem

According to Haddow et al. (2021), the United States has experienced an increase in acts of domestic terrorism and acts of violence that involve violent extremism and radicalization, including behaviors such as violent shootings, bombings, violent physical attacks, gang beatings, arson, lynching, vandalism, and property destruction. Haddow et al. explained that over the past five years, communities have experienced domestic threats and taken measures to prevent, prepare, and respond to acts of domestic terrorism. The term “terrorism” encompasses extremist activities involving specific ideologies, tactics, and weapons, including bombings, improvised devices, mass shootings, chemical and biological agents, and physical assaults (Haddow et al., 2021). Further, Haddow et al. stated the Natural and Technological Hazards and Risk

Assessment also identifies weapons of mass destruction as chemical, biological, or radiological weapons. In the United States, domestic terrorism encompasses activities and actions that are dangerous to human life, violate U.S criminal law or laws of a state, and involve measures designed to intimidate the government and influence a government policy and the political process. Haddow et al. recounted that Timothy McVeigh and Terry Nichols conducted a domestic terrorist attack on the Alfred P. Murrah Federal Building in Oklahoma City and considered it to be the most devasting domestic terrorist attack in U.S. history. According to Haddow et al., the perpetrators "claimed the U.S. government had overstepped its bounds regarding gun control and in its handling of the Ruby Ridge, Idaho, and Waco, Texas standoffs" (p. 416).

Purpose of Study

This dissertation research study is aimed to shed light on the importance of PRAs in critical infrastructures, homeland security, and social elements. The goal is to provide data, statistics, and guidance to help secure critical infrastructure and key resources involving electric grid power systems, natural gas pipeline distribution, and natural gas transmission in communities. The study will address the problems that can devastate society, human life, government, economic and financial sectors, emergency services, and other resources to explore the benefits of PRAs in society from a theoretical perspective. Kumar et al. (2021) stated that a novel framework for conducting a PRA on critical infrastructure should include assessing the impact of climates changes, especially in areas where an event can impact communities (e.g., fires, hurricanes, tornados, and flood-prone areas) and population changes that impact local emergency services and resources. For example, risk assessments are essential in building resiliency in infrastructures in areas where there is extreme precipitation and drought because

PRAs provide planners and policymakers with the ability to ensure new development will be based on data, statistics collected, and on principles of flexibility, diversity, consideration given to industrial ecology, and develop an understanding of short-term and long-term impacts of climate risk (Kumar et al., 2021).

Forman (2020) noted that in countries such as the United Kingdom and the United States, extensive natural gas infrastructure and natural gas transmission lines exist, and dangers associated with the subterranean and underground circulation of natural gas express the need to provide adequate security. In 1985 in the United Kingdom, there was an explosion which “killed eight people, demolished six apartments, and shattered all nearby windows within a quarter of a mile radius [and involved the] 7600-km-long National Transmission System” (NTS; Forman, 2020, p. 146), which is part of the natural gas national grid system. Forman noted the NTS consists of a transmission system responsible for transporting a large volume of natural gas throughout the country at high pressure to producers, international interconnectors, and delivery to specific regions and lower gas pressure to consumers. Natural gas movement and transmission have geopolitical implications and adequate security is required to protect the NTS (Forman, 2020). In addition, public safety has an increased role in securing energy supplies in society. Forman further suggested that management and security professionals should recognize the importance of securing natural gas movement, identifying risks and points of vulnerability, and providing intervention to help ensure the environment and communities because of the nature of subterranean and underground natural gas infrastructure. The proposed dissertation will briefly examine four trajectories related to the management, transmission, distribution, and movement of natural gas at the subterranean level and measures to protect and secure these critical infrastructures from acts of domestic terrorism and other risk and vulnerabilities.

Importance of Study

Natural gas and propane are essential resources in metropolitan and rural areas. Natural gas distribution and transmission are critical infrastructures that provide the help needed in electricity generation to meet basic human needs in communities to prepare meals and to provide heat and hot water. The proposed study is important because it will examine how to prevent and protect these critical infrastructures from risk, vulnerabilities, and domestic acts of terrorism. The dissertation's research involving critical infrastructure, homeland security, domestic terrorism, extremism, and transformational leadership will provide research theories to address each quantitative research study element. Another goal is to contribute to future research in mitigating risk and vulnerabilities associated with critical infrastructure and key resources applicable to other infrastructures. The dissertation will provide a quantitative research study on managing natural gas critical infrastructure and transmission and securing these vital infrastructures. Scripture teaches that "It is the glory of God to conceal a thing, but the honor of kings to search out a matter" (*King James Bible*, 1769/2021, Proverbs 25:2).

According to Beyza et al. (2019), a theoretical approach to managing critical infrastructure and vital resources includes graph theory and network theory. These theories are an approach designed to evaluate processes that have been cascading system failures. The process will require networking and conducting statistical analysis using "statistical indexes applied from elements of graph theory" (p. 1). During the procedure, management undergoes a network series process to determine the cascading failures and conduct simulations and a "statistical analysis by testing natural gas test networks" (Beyza et al., 2019, p. 1). These are theoretical approaches designed to help management minimize downtime, analyze stand-alone systems, and evaluate power systems that control the flow of natural gas. The quantitative dissertation research study will explore the drivers for change and research gaps, contribute to future research, and examine the role of PRAs in government and management structures in protecting critical infrastructures and key resources in society. In the spiritual domain of inflow of spirit, Scripture teaches, “It is the Spirit that gives life and the flesh profits nothing; the words I have spoken to you are spirit and life” (*King James Bible*, 1769/2021, John 6:63).

CHAPTER TWO: LITERATURE REVIEW

Overview

This chapter encompasses the literature review that addresses PRAs in critical infrastructure and homeland security. The chapter includes defining the role of this type of risk assessment in homeland security, examining factors relevant to protecting electric power grid systems' and natural gas pipelines' critical infrastructures from domestic terrorism, an increase in violent extremism, and developing a framework based on probabilities in counterterrorism processes. Leaders must be prepared to safeguard and secure critical infrastructures such as natural gas pipelines and electric power grid systems, and other vital resources from domestic terrorists, violent extremists, lone wolf actors, and natural and manufactured disasters in the homeland security profession. The dissertation will consist of a quantitative research study on PRAs in homeland security and valid research on these three manageable issues related to domestic terrorism, violent extremism, and protecting critical infrastructures such as natural gas pipelines and electric grid power systems.

According to Chatterjee et al. (2021), a PRA is a methodological and systematic approach designed to evaluate complex risk. It assesses the probabilities of other risks and vulnerabilities by seeking answers to questions such as what can potentially go wrong, examining the likelihood of an event, occurrence, or phenomenon, and what probable measures can be taken to mitigate concerns. In PRAs, this type of risk assessment process is formulated to help evaluate, identify, and measure current and future trends through metrics designed to be used by agencies and organizations in homeland security in specific models, solutions, and scenarios, and to track specific trends, extreme weather events, domestic terrorism activity, and cyberattacks (Chatterjee et al., 2021). Furthermore, Chatterjee et al. explained that elements of government, the private sector, and society in general, PRA provides leaders with guidance and tools to evaluate certain factors and risks by providing reliable knowledge on uncertainties that require special consideration and considering probability spaces.

Grimmett (2021) described that a scenario-driven model could include known and unknown factors in socio-security systems. According to Grimmett, these systems can involve multiple stakeholders and multiple factors that may present additional challenges if consideration is not given to macro-scale disruptions in security, demographics, politics, and the environment in a multicriteria analysis. In scenario-driven models, risk management can include a framework that considers probability versus consequence can be highlighted on a graph or use metrics to illustrate factors relevant to the risk assessment associated with low, moderate, significant, and high risk (Grimmett, 2021). Probability is a factor that can be applied in many areas such as emergency response, energy applications, assessing consequences, assessing behavior, fitness, terrorism, and violent extremism. In Chapter Three, different methodological approaches will be discussed in detail.

According to Durrett (2019), probability can also be viewed as a measure or measurement theory that identifies probability as space-related factors. It relates to factors associated with a set of outcomes, consequences, events, and functions highlighted as a three-part process and illustrated in a field and mathematical process. Outcomes in probability theory can be conceived as an experiment, event, trial, test, or scenario, with each having a different outcome. In equations, the probability is generally highlighted and represented as "P or as $P(A)$ as the probability of a function $P(A) = 0.5$, and probability introduced where events intersect is represented by $P(A \cap B)$ or $P(A \cap B) = 0.5$ and probability illustrated as an event union is represented by $P(A \cup B)$ or $P(A \cup B) = 0.5$" (Durrett, 2019, p. 1).

According to Holzmann and Smith (2021), in homeland security and the military, when addressing challenges and problems in the organization, leaders must select the shortest path to interdiction that may involve a zero-sum game and selecting a strategy directed toward problems in a specific area of concern. The interdiction strategy may include formalities designed to take into consideration metrics that include a set of arcs and costs. Holzmann & Smith suggested that leaders must select the appropriate path which maximizes benefits in the followers' cost. However, followers must also select the minimum cost and path to achieve goals and objectives. In this case, when leaders and followers select an appropriate strategy, probability is a factor that is part of a "policy of randomized interdiction actions" (Holzmann & Smith, 2021, p. 82) when selecting a specific course action to address challenges and problems. Holzmann & Smith further suggested that PRAs can provide leaders and followers in homeland security and the military with specific options based on assessing the shortest path in interdiction strategies to approach specific problems and solve linear problems.

Modern PRAs have been around since the 1980s and are used in the nuclear industry to assess risk (Standley et al., 2020). It is a risk assessment process that is used to assess detection processes and complex warning systems in elements of risk reduction. Standley et al. (2020) explained that probabilities are used in risk assessments and decision-making in military wars and are a significant part of the leadership in assessing risk. According to Standley et al., the "likelihood ratio test (LRT), based on Bayes' theorem" (p. 137), is a process used to assess the probability of an observed outcome. However, there must be a basis for probability before the LRT is applied. The probability of severity must be equal to the consequences of computing risk. The proposed research will highlight data on how probability functions in various scenarios and from a cloud perspective in assessing risk. Research suggests there is still a strong need to understand the research gaps in homeland security and wars in how probabilities are used to focus on specific problems in decision making, and detection, and how it is used to compute and minimize risk and risk reduction by “fusing detection information and war statistics” (Standley et al., 2020, p. 1387).

According to Abreu et al. (2019), in measuring probability in homeland security related to incidents involving violent extremists and mass shootings, the new stochastic model can be used to maximize survival probabilities by identifying the potential characteristics of people that may be involved in these situations. In addition, it includes understanding patterns in the behavior of the perpetrators or shooters’ effectiveness. Abreu et al. noted it is essential to understand probabilities related to the impact human parameters have on mass shooting attacks and an individual ability to overcome a shooting incident to save lives while putting themselves at a greater risk. Abreu et al. further suggested that a good starting point is based on applying stochastic simulations to understand key human parameters to increase survival probability, which can involve exploring probable measures to improve self-protection and explore ways to increase interactions and simulate processes by creating scenarios. In the homeland security and criminal justice system exploring probability in various scenarios can involve examining outcomes from the bottom up rather than through prescribed measures and modeling tools. The goal is to create more accuracy, increase simulation times, and explore probabilities in real time (Abreu et al., 2019).

According to Suo et al. (2021), PRAs for critical infrastructure are conceived as quantitative measurements for assessing the probability of an occurrence associated with a specific risk profile that emerges and identifying weaknesses in informal processes. The risk associated with critical infrastructure and key resources is often more challenging and problematic because there is interdependency and a multiplicity of risks among some infrastructures. Because of the dynamic stochasticity of some critical infrastructure, and when a PRA is more challenging, it will require more procedures. Suo et al. suggested that a stochastic model can require three stages to provide a more accurate depiction of risk to qualify for the assessment. First, the PRA requires the use of factual, objective records and must be submitted to the subjective judgment of experts to qualify as part of the assessment. Suo et al. noted that this type of model can apply to decision-makers in many cases and is required in public policy to provide an adequate and thorough risk profile. Furthermore, risk can be modeled to highlight the level of risk (low, moderate, or high), determine the frequency of risk, and help to determine the frequency in which risks are more prevalent or highlighted during specific periods of risk.

To conduct a risk assessment on critical infrastructure, two elements must be included in a scenario that can involve the use of "multiple risk factors and multiple interdependent critical infrastructures" to determine the multiplicity (Suo et al., 2021, p. 107730) p. 1). First, respectively assessing each infrastructure, a determination must be made on a specific level or period of risk. Risk factors related to multiplicity involve factors related to operational functions, hydrometeorological hazards, domestic terrorism, down power lines, and pipeline failures. Factors related to critical infrastructure interdependency are associated with spatial proximity, material exchange, and how some infrastructures are interwoven and utilize the same communication and system networks, according to Suo et al. (2021). Dynamic stochasticity risk factors refer to how infrastructures can be impacted by different risk events that, on the other hand, can then impact operational functions. When critical infrastructures are susceptible to more risk, there can be variations and uncertainty. Suo et al. further explained that the end goal of a PRA related to critical infrastructures is risks that must be quantified by probability and loss.

When a PRA is required to measure weaknesses, it is based on several factors relevant to whether weaknesses have been determined by the risk periods of alert and based on a higher frequency of risk factors, mitigation, and preventive measures. These are factors that will be discussed in detail in Chapter Three as part of the methodological processes.

Karbowski et al. (2019) noted in homeland security and national security, the risk associated with cybersecurity is a significant concern for leaders and the private sector. To mitigate these concerns, the Markov chain model can be used to assess the probability of distribution to assess risk related to the future state of operational performance of system networks. This is a process that involves the concept of detection and preventative measures designed to provide data and information on probabilities and unforeseen events that have not occurred, but can predict and evaluate future consequences related to an event capable of disrupting system networks. Karbowski et al. suggested it is a process that shares similarities with the Bayesian network model by compiling data on smaller directed acyclic graphs (DAG). PRA related to this model will also be referenced in Chapter Three.

Critical infrastructure and key resources are provided with guidance and special protection in homeland security. According to Newbill (2019), a Google search of the phrase “critical infrastructure” yields “189 million results in little more than a half-second, and global critical infrastructure results would illustrate 151 million, and how critical infrastructure is defined will provide 71.5 million results” (p. 761). Newbill asserts that the number of critical infrastructures has increased because industries, sectors of critical infrastructures, and new advancements in technology have expanded due to new communications systems and operational functions and the need to provide resources for basic human needs as well as to support economic development and government needs. Furthermore, Newbill noted that some boundaries related to critical infrastructure constitute a need for additional measures in physical protection and cybersecurity on a global and international level. The type of protection given to infrastructures relies on the threat landscape, risk, vulnerabilities, and limitations identified to determine the significance of national and global infrastructures. In homeland security, a significant focus is on cybersecurity and placed on nation-state actors capable of hacking into facilities, networks, and systems that control critical infrastructures (Newbill, 2019).

According to Herring (2020), in conducting a quantitative literature review on homeland security, the theoretical probability can involve equations, analyzing phenomena and mathematical statistics, data, angulation, and assessing an occurrence, incident, or event. To explore how effective a homeland security framework (HSF) is in emphasizing an organizational approach and design to guide risk assessment and "enhanced operational integration and collaboration across America's (HSE) (Herring, 2020, p. ii). Herring further noted that PRAs could provide quantitative data to examine current themes and trends in homeland security and collect data from agencies within departments of homeland security, data on organizational behavior, and the type of research instruments designed to "collect and analyze descriptive data to answer the research questions" (p. 9). This dissertation literature review has significant sections on homeland security and the three manageable issues identified as mitigating domestic terrorism, extremism, and counterterrorism efforts. According to Herring, a significant emphasis is on protecting and securing a natural gas pipeline's critical infrastructure and other essential resources in a local area that can be impacted by acts of terrorism and domestic terrorists.

According to Knight and Gekker (2020), in homeland security, critical internal infrastructures function to provide government support with technological advancements responsible for surveillance and data analysis software. Knight and Gekker suggested the goal is to support how the United States manages processes involved in immigration and elements of national security (p. 231). In homeland security, a theoretical framework in a government infrastructure can include “Benjamin Bratton’s concept of the interfacial regime, used to interface with the ‘Investigative Case Management (ICM), a system designated to provide support for the Immigration and Customs Enforcement (ICE.).” (Knight & Gekker, p. 231). A technological process is used to conduct data analysis to help track immigration processes; oversee, manage, and enforce immigration policies; help to avoid governmental abuses, and support U.S. homeland security and national security systems.

In homeland security, Wilcox (2020) noted that leadership must mitigate domestic terrorism, prepare for threats posed by actors engaged in information warfare and data breaches, and enhance counterterrorism measures necessary to meet today’s challenges. Wilcox suggested that in mitigating these challenges, under the National Security Council (NSC) Information Warfare Directorate (IWD), leaders must take necessary measures and provide analysts, leaders, and policymakers with practical recommendations to implement policies on mitigating domestic terrorism and extremism threats and protecting critical infrastructure (p. 111). Wilcox further noted that effective leadership is essential in establishing robust domestic and foreign policy and representing foreign interests. In homeland security and national security research, information and communication technologies must be more adequately prepared for information warfare in the near future. Homeland security research in the future must also focus on the U. S. adversaries’ ability to convert from “conventional warfare (CW) to non-conventional warfare (NCW)” (Wilcox, 2020, p.108).

Strang (2018) stated that effective leadership is essential to the success of homeland security. Leaders must engage in strategic planning to plan for unexpected risks, vulnerabilities, and threats to infrastructures and organizations' performance. Succession planning is an essential part of the selection process and selecting leaders to fill critical positions in the not-for-profit (NFP) organization. Strang stated that NFPs must approach threats based on threat assessments, best practices, and risk management activities to mitigate threats. NFP organizations that participate in elements of homeland security must also conduct security checks on staff and volunteers to determine if potential employees are on the DHS national terrorism blacklists and no-fly-watch list, according to Strang.

According to Brod (2018), effective leadership involves communicating the vision change initiatives designed to impact the organization, organizational structure, and subordinates in the homeland security agency. In a quantitative research study, future research should focus on "leadership skills on readiness for change" to provide a comprehensive approach to leading organizational change (Brod, 2018, p. 108). In one research study, Brod further noted the goal was to help create new knowledge to contribute to future research and create research design toward a "willingness to accept and promote change within the organization" (p. 108). In homeland security, agency leaders must recognize the following:

- Protecting critical infrastructures and key resources such as natural gas pipelines, electric power grid systems, and water treatment facilities is essential.
- Community policing and law enforcement are essential in homeland security and critical in counterterrorism in collecting data on potential domestic threats.
- Law enforcement provides a system to collect critical data applied in counterterrorism efforts.
- According to some theories, two means of "transforming input into output" are accomplished by (Brod, 2018, p. 37):

- A determination is made on “who transforms the information through the political process” (Brod, 2018, p . 37).
- Cultural norms are “transformed into outputs” to improve outcomes (Brod, 2018, p. 37).

Wibeck et al. (2019) suggested that societal change is often a driver for change in leadership, and societal transformation may include exploring the environment, sustainability, and processes to address global challenges. Societal change may require leaders to examine nonlinear systemic processes related to “climate changes, rapid urbanization, increasing energy demands, and pressing need for poverty reduction” (Wibeck et al., 2019, p. 2). Further transformative changes in homeland security research may examine the impact of individual factors, formal settings, and goals and create pathways towards change based on “geographical, socioeconomic, political, and cultural” dynamics (Wibeck et al., 2019, p. 2). Furthermore, Wibeck et al. noted some researchers seek to examine the relationship between transformation, sustainability, and what drives societal change, defining critical conditions for change and identifying change agents. Wibeck et al. also suggested a theoretical approach in future research to understand how social change occurs is to examine social systems, the period for change, the scope of transformation, and identify the drivers and agency.

Steckler and Waddock (2018) suggested that in elements of homeland security, transformative changes may include developing a framework that recognizes three factors or retreats associated with “reflective, relational, and inspirational” aspects of leadership (p. 171). These factors are essential in providing sustainability for change agents and transforming leaders. When there is a cultivation of transformative retreat leaders, Steckler and Waddock further suggested they will develop perseverance, resilience, and focus on personal well-being.

Humanity becomes a priority in transformative change, and leaders create the ability to "achieve success in their transformational endeavors" (Steckler & Waddock, 2018, p. 171). Inspirational practices are essential in dealing with day-to-day challenges, societal change, and threats relevant to homeland security in a leadership role (Steckler & Waddock, 2018). Passionate worship allows leaders to create and develop a place and space for enlightenment, spiritual development, and reflection. Scripture teaches, "The Lord provides blessings to all, according to the riches of his glory, as a way to strengthen man by his Spirit in the inner man, and Christ dwells in the hearts of men through prayer and faith; that ye, being rooted and grounded in love" (*King James Bible*, 1769/2021 Ephesians 3:16-17).

U.S. Department of Homeland Security

The U.S. Department of Homeland Security was created, after September 11, 2001, in response to acts of terrorism and terrorist attacks committed on U.S. soil. The DHS consists of 11 agencies or components. It is a federal agency with a mission to protect the United States from domestic and international terrorist threats. Federal agencies such as the Federal Emergency Management Agency (FEMA), Drug Enforcement Administration (DEA), U.S. Secret Service, and the Federal Bureau of Investigation (FBI) have a broad range of responsibilities, including interdiction, counterintelligence, counterterrorism, aviation security, border security, emergency response, and protecting critical infrastructures and key resources. An essential mission of homeland security is enhanced security and the prevention of acts of terrorism. Domestic terrorism includes violent extremists, anarchists, lone-wolf terrorists, and acts of terrorism committed on U.S. soil, where the FBI is the lead agency that responds to and investigates terrorist-related incidents. Citizens around the country saw violent domestic extremism in the U.S. capital on January 6, 2021, which shook the country, government, and the political landscape.

According to Hunter et al. (2020), in some democracies, internet connectivity plays a role in domestic terrorism, violent extremism, and lone-wolf terrorist activities. The internet is seen as a channel for potential terrorists to communicate and spread propaganda. Hunter et al. noted that in some democracies, the internet is the channel to share extremist views, ideologies, and radicalization. The internet and social media serve as a platform for radicalizing and recruiting individuals into domestic and international terrorist groups and organizations. Further, Hunter et al. suggested it is not easy to measure radicalization in many democracies because different regimes or authoritarian governments support political processes and institutions in other countries. In the United States, domestic terrorism may be examined and studied from three different perspectives:

1. Determine the impact propaganda has on the radicalization process and terrorist recruitment.
2. Conduct theoretical studies on how social media and the internet may be associated with 'domestic terrorism in democracies,'
3. Conduct research studies on democracies likely to have “greater incidents of domestic terrorism” based on demographics and internet reach (Hunter et al., 2020, p. 202).

Hunter et al. suggested another essential factor in determining how internet usage supports domestic terrorism is propaganda used to “spread extremism ideologies, recruit new members, and carry out attacks” (p. 202). To determine these factors, future research should focus on how different internet platforms may support domestic terrorism and violent extremist ideologies. Future research should also examine social media outlets' role in influencing the radicalization process, recruiting new members, and spreading violent extremist propaganda, polarization, and self-radicalization processes. Hunter et al. further stated that future research should examine the psychological impact the internet may have in influencing conflict and terrorism.

According to Brogan et al. (2020), how domestic terrorism and counterterrorism are perceived in the United States has changed due to the results of the 2016 presidential election and leading up to the 2020 presidential election. Some believe “electoral campaigns have demonstrated that politicians are actively trying to politicize terrorism” (Brogan et al., 2020, p. 1). There have been new challenges in counterterrorism in the United States because of the rise of violent extremism, left and right extremist movements, and how some may view the Blue Lives and Black Lives Matter (BLM) movements. When domestic terrorism becomes politicized, violent extremism increases and many nonviolent movements around the country become infiltrated by violent extremists and pro-government groups. These groups have also received support from specific political parties on both sides of the political spectrum. When violent extremism and particular groups are polarized, it creates a recipe for civil unrest. Brogan et al. noted the “danger of politicizing terrorism” (p. 1) blocks finding common ground in parts of society; once this occurs, people become radicalized and entrenched in extremist movements. These acts of violence are often against the U.S. government, political process, government policies, and law enforcement. Domestic terrorism events and violent extremism impact homeland security and counterterrorism elements and how people view the political process and the government’s ability to protect against domestic terrorist groups and acts of terrorism. Domestic terrorism is often supported; by selected ideologies, tactics, causes, and violent extremist organizations that operate under the guise of white supremacy and militias.

"Ideological motivations of terrorists" and extremist groups' motivations are directed toward dismantling governments and influencing voters (Brogan et al., 2020, p. 1).

Brogan et al. (2020) suggested developing an understanding of domestic terrorism in homeland security and the essential dynamics in the profession and counterterrorism in protecting critical infrastructures such as natural gas pipelines, communication technology, and first responder personnel. In addition, these domestic terrorist groups' activities create "internal and external security challenges" and threats in the U.S. and raise counterterrorism concerns (Brogan et al., 2020, p. 2). Finally, Brogan et al. explained that citizens in the country have conflicting views on the government's ability to prevent future terrorist attacks. Therefore, future research on these subjects should focus on specific areas of concern:

- How political partisanship can have an impact on counterterrorism policies and in shaping perception.
- The negative impact that politics or political campaigns can have on domestic terrorism, counterterrorism, and threats to critical infrastructures; and
- Race and national origin can have an impact on responding to terrorist threats.

Homeland security and counterterrorism rely heavily on information input from collecting data and information obtained from various intelligence sources. Brogan et al. explained that this might include "problem locations, gang activity, affiliation to terrorist organizations, weapons used, arrests, and prison releases" (p. 33) concerning extremists and anarchists.

The information input process is vitally important to mitigate potential threats and develop counterterrorism strategies to respond to threats. From a homeland security perspective, law enforcement has a critical role in collecting data and information on individuals deemed as actionable intelligence or probable domestic threats to reduce domestic threats and extremism in the United States. According to Brogan et al. (2020), in the United States, between 1987–2010, law enforcement was credited with mitigating 73% or 83 potential domestic terrorist plots and thwarting 89 domestic terror plots; furthermore, “66 were foiled through human intelligence (HUMINT) from members of the public, covert police operations, or police informants” (p. 5). However, in the United States, many law enforcement agencies have a problem engaging in proactive counterterrorism activities to collect data and information on domestic terrorist and extremist groups engaging in counterterrorism activities and developing counterterrorism strategies and tactics.

Under the DHS (2021), the National Terrorism Advisory System (NTAS) serves as a warning system when there is a heightened domestic terrorism “threat environment across the country” (p. 1). The NTAS provides a bulletin on new developments and threat trends. The current threat environment involves ideologically motivated, violent extremists. According to the DHS (2021), these extremists object “to the exercise of governmental authority and the presidential transition” (p. 1). The current threat assessment suggests extremist terrorists in the United States pose a credible threat. The current threat environment consists of the following:

1. Targeting individuals who oppose views related to the “First Amendment-protected, non-violent protest activity,” and anger-fueled over COVID-19 restrictions, 2020 election results, and police use of force.
2. Violent protest over “racial and ethnic tension” and views on immigration.
3. Foreign terrorists inspire homegrown violent extremists (HVEs).
4. Violent extremist threats are directed toward critical infrastructures, electrical grids, and telecommunications infrastructures.

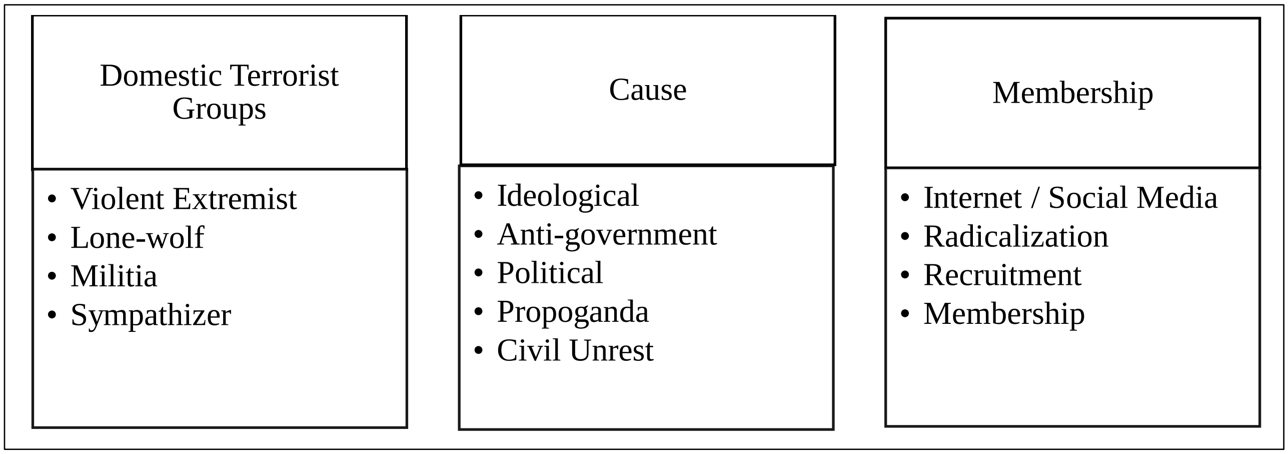
5. Threats are meant to intimidate or coerce based on religious views, race, ethnicity, identity, or political beliefs.

The DHS (2021) has emphasized strengthening security measures and prioritizing physical security measures to protect people and critical infrastructure.

The DHS noted that in 2020 and 2021, a primary goal of homeland security and the NTAS is preparedness and preparation to prevent the spread of COVID-19 and the Omicron surge and prevent domestic terrorist incidents. A formal process designed to conduct a Homeland Security Threat Assessment to inform the public of current and pending threats. The DHS encourages citizens, partners, and stakeholders "to report suspicious activity and threats of violence" (DHS, 2021c, p. 1). to include reporting online threats to local FBI offices, fusion centers, and local law enforcement agencies. The DHS encourages supporting communities and "if you see something, say something" to help prevent acts of domestic terrorism.

Figure 1

Domestic Terrorism Dynamics



Domestic Terrorist Groups	Cause	Membership
• Violent Extremist • Lone-wolf • Militia • Sympathizer	• Ideological • Anti-government • Political • Propoganda • Civil Unrest	• Internet / Social Media • Radicalization • Recruitment • Membership

According to Guhr et al. (2019), homeland security, national security, and securing critical infrastructure and key resources are at the forefront of homeland security in the security profession. Today, many challenges and problems are often associated with mitigating threats related to domestic terrorism, extremism, and improving counterterrorism efforts. Domestic terrorism is often supported by selected ideologies, tactics, causes, and violence. Guhr et al. suggested that effective leadership is essential in information security because leadership and management directly impact information security behavior and other areas of homeland security. Leaders can often influence subordinates and improve “extra-role and in-role behavior levels [and] full-range leadership theory” provides theoretical and empirical sound guidance on leadership approaches (Guhr et al., 2019, p. 340). A goal is to help employees rise above self-interest to change and motivate employees to perform better and achieve their goals and mission.

Goswami et al. (2018) suggest many problems are related to the drivers of domestic terrorism and changes in leadership. As a result, homeland security and law enforcement agencies have experienced many challenges and difficulties. First, leaders must create “corporate social responsibility” and a positive image (Goswami et al., 2018, p. 645). Second, leaders must develop transformative measures to help improve society, create better opportunities for employees, and communicate more effectively with communities in “adhering to legal regulations” and the letter of the law (Goswami et al., 2018, p. 645). Third, a leader must examine organizational and citizenship behavior factors to address unethical behavior problems and the need to build strong collaborations and foster cooperation, friendships, trust, acceptance, and fellowship. Finally, Scripture teaches, “But if we walk in the light, as he is in the light, we have fellowship one with another, and the blood of Jesus Christ, his Son, will cleanse us from all of our sins” (*King James Bible*, 1769/2021, 1 John 1:7).

Fiebig and Christopher (2018) suggest that women play a unique role as leaders in homeland security and the community, and an example is a role women play in the "intersection of Catholic women works" as sisters and church leadership (p. 505). Women have served in unique roles in the religious community and have represented servant leadership styles. Fiebig and Christopher noted that the skills many women possess are an asset to an organization and organizational structure. In the religious community, women identified as leaders have outstanding leadership qualities that center around five trends:

1. These leaders show a willingness to possess "significant leadership responsibilities,"
2. In many cases, women are more caring and "compassionate towards others,"
3. Women in servant leadership roles possess skills necessary to help guide an "individual towards personal growth,"
4. Women often serve as great role models,
5. Women in transformational-servant leadership roles possess the ability to "create solutions to social justice issues and security problems" (Fiebig & Christopher, 2018, pp. 505, 509, 512).

The proposed research will also focus on women's role in transformational-servant leadership roles in homeland security and the impact of spirituality and religion on management styles. Fiebig and Christopher suggested another goal is "to examine future women's religious management styles by explicitly highlighting the use of servant leadership" as a model for spiritual support (p. 512). The dissertation will also address the research questions related to Christian perspectives on many challenges and problems in homeland security. For example, Scripture teaches, "It shall not seem hard unto thee when thou send him away free from thee; for he hath been worth a double hired servant to thee, in serving thee six years: and the Lord thy God shall bless thee in all thou do" (*King James Bible*, 1769/2021, Deuteronomy 15:18).

Three Manageable Issues

Domestic Terrorism

Many of the challenges and problems in homeland security related to domestic terrorism and violent extremism require local law enforcement authorities and counterterrorism professionals to respond to threats. Domestic terrorist groups such as violent extremists, anarchists, White supremacists, and lone wolves have been designated domestic terrorist groups and organizations in the United States and local municipalities. Piazza (2020) explained that domestic terrorism is propagated in many parts of society by political rhetoric and can include hate speech and "rhetoric that targets, vilifies, excludes or is fashioned to intimidate racial, ethnic, religious or sexual minorities, women, political opponents, migrants, disabled persons or members of other groups by political figures fuel domestic terrorism" (p. 431). Piazza further noted that the use of hate speech and rhetoric associated with the political climate appeals to some domestic terrorists, and acts of violence are not limited to past mass shooting incidents, nor are they limited to America. Discriminatory rhetoric linked to political activity or the political environment can increase the potential for domestic terrorist attacks.

Domestic terrorists often share extremist viewpoints but have different ideologies and are a threat to the U.S. government, and these groups also pose a threat to local communities, law enforcement, electric grid power systems, and natural gas pipeline infrastructures. Many local police organizations face multifaceted challenges, community problems, increased public scrutiny, and domestic threats. In 2020, the increased police shootings, civil unrest, and demonstrations attracted many domestic terrorist groups. These problems led to extremists infiltrating many peaceful protests and raising the homeland security threat level on domestic terrorism. These groups have also become a threat to local critical infrastructures and government buildings. Another homeland security threat in the United States and other countries is the COVID-19 pandemic, stretching homeland security and law enforcement resources to the limit and creating a virtual environment. In September 2020, several demonstrations and problems in law enforcement and homeland security events increased the COVID-19 threat environment in the United States and the need for transforming organizations and changes in how many businesses do business and function.

According to Laguardia (2020), in the current domestic terrorism environment, many in the criminal justice system and public and legal practitioners feel the need for a “domestic terrorism statute,” one designed to eliminate disparities between domestic and international terrorism (p. 1061). Laguardia suggested prosecutions for international terrorism charges involve material support, terrorist acts prohibited by law, and designations associated with international terrorism. In law enforcement, there are hurdles in prosecuting domestic terrorists. Laguardia further suggests the disparity in terrorism cases involving international terrorism and domestic terrorism is that domestic terrorism prosecutions are rare. In criminal prosecutions involving international terrorism, “terrorists receive longer sentences and may be subject to more aggressive investigations with less oversight” (Laguardia, 2020, pp. 1064–1065). In addition, domestic terrorism associated with violent White supremacists is classified as a hate crime in most cases. Laguardia further noted prosecuting domestic terrorism will require a federal statute to charge designated domestic terrorist groups and organizations as domestic terrorists to address the gap in the federal statutory framework.

Laguardia (2020) pointed out that there are disparities among law enforcement in how international terrorism cases are prosecuted in federal courts compared to domestic terrorism cases. Due to the rise in right-winged extremist violence and domestic terrorism, there is a call for the federal government to create a domestic terrorism statute. With the increase in domestic terrorist activity, domestic terrorist statutes should swiftly eliminate barriers to prosecuting these cases. The problem with prosecuting domestic terrorism cases in the United States is that there are general statutes for acts of terrorism, and these cases can be highly problematic. Depending on the act, laws used to prosecute domestic terrorists do not apply to prosecuting international terrorists. Laguardia further suggests more statutes should lessen disparities and mitigate how right-winged extremist terrorists and other domestic terrorist cases in the United States are prosecuted and pass stricter laws.

Laguardia (2020) noted the example of a 2018 FBI case that involved members of the Rise Above Movement (RAM), a White supremacist, neo-Nazi gang engaged in violent behavior in Charlotte, South Carolina, and charged members in a “criminal indictment for actual violent conduct” (p. 1061). However, in this case, members of the terrorist organization will not face terrorism charges. The information further suggests a White supremacist named James Alex Fields, Jr. was also responsible for Heather Heyer’s death during the protest, and domestic terrorists are rarely charged (Laguardia, 2020). International terrorist charges under the terrorist statutes receive longer sentences, and investigations are more extensive. Federal laws concerning terrorists and terrorism do not cover domestic terrorism according to how international terrorists are treated under U.S. laws.

According to Berryman (2020), social media providers should be held accountable for facilitating acts involving domestic terrorism and the “availability of a federal cause of action”

(p. 1329). Still, it might dissuade domestic terrorists and violent extremist groups from engaging in such activities. An obstacle may include proving a proximate cause of action and establishing the connection between domestic terrorists and social media. In addition, this also includes establishing a social media outlet cause of action directly linked to domestic terrorism or the actions of domestic terrorists. Moreover, victims of acts of domestic terrorism face obstacles. Even though the Antiterrorism Act of 1990 (ATA) includes "civil remedies for international terrorism" (p. 1329), when acts of domestic terrorism or international terrorism occur, victims have little chance of recovering any damages.

Krueger et al. (2020) explained that in the current domestic terrorism threat environment in the United States, some feel domestic surveillance is a balance between liberty and security. In some cases, domestic counterterrorism policies and surveillance are too intrusive, even though these policies are designed to improve safety and security. Krueger et al. suggested the increase in counterterrorism efforts has led to a rise in domestic terrorism and framed it as a trade-off between "core political values or whether they depend on the messages from political leaders" (p. 104). In one study conducted in Europe concerning balancing privacy and security, Krueger et al. noted that enhancing domestic security does not reduce security efforts. Future research should assess whether the security-liberty trade-off impacts individuals' personal beliefs or shapes views in specific contexts if individuals are willing to conform to changes in security policies. Krueger et al. further noted political affiliations in counterterrorism cases feel these policies align with more "political predispositions and existing knowledge" (p. 105).

According to Gaibulloev and Sandler (2019), terrorism is defined as the premeditated use or threat of violence by individuals or subnational groups against noncombatants, and the goal is "to obtain a political objective through the intimidation of an audience beyond that of the immediate victims" (p. 331). In viewing domestic terrorism from a political perspective, Gaibulloev and Sandler noted domestic terrorism often occurs in other countries with relationships with the United States or key Western countries with more transnational and domestic terrorist attacks. In some cases, U.S. allies or affinity-lined relationships some countries have with the United States make some countries more susceptible to domestic terrorist attacks. In some countries, because of the diplomatic relations between the United States and three countries, they further noted that France, Germany, and the United Kingdom have contributed to domestic terrorism.

Gaibulloev and Sandler (2019) described domestic terrorism as a phenomenon that involves homegrown terrorism and acts of violence perpetrated by violent extremists. In many cases, the victims and perpetrators are often citizens living in the country. Some are often locally-based and share propaganda and misinformation with other domestic terrorist organizations. In most cases, domestic terrorists are politically motivated and engage in violent acts against citizens, the government, and law enforcement. Gaibulloev and Sandler further stated that there are far more domestic terrorist attacks than transnational terrorist attacks, and struggles leading to domestic terrorist attacks are considered "domestic terrorist incidents" (p. 332).

In a review of an article in *The Washington Post*, McAleenan and Plofchan (2020) noted that the DHS issued the "first annual release on Homeland Threat Assessment" (p. 1) in 2020. The report categorizes domestic terrorists as "ideologically motivated lone offenders and small groups of violent domestic extremists" as the leading threat in America (p. 1). These organizations pose the greatest threat to the way of life, the business community, and civil liberties. During the November 2020 election, McAleenan & Plofchan suggested domestic terrorist groups were responsible for heightened social and political tensions and used the infringement of civil liberties as an excuse for violent extremist actions during the initial response to the COVID-19 pandemic response.

McAleenan & Plofchan further suggests in perpetuating violent extremist activity, other lone-wolf actors and organized domestic terrorist groups use the internet to spread propaganda and misinformation and accelerate the velocity of radicalization and violent actions. Today, the challenges posed by domestic terrorist groups and lone-wolf actors require an all-hands-on-deck approach to mitigate violent extremism. McAleenan & Plofchan noted federal agencies such as the FBI engage in activities to investigate domestic terrorism and investigate any foreign influence. In addition, the U.S. Secret Service analyzes domestic terrorism and guidance to prevent mass attacks. Finally, the Cyber Security and Infrastructure Security Agency provide support to nonprofit agencies and communities to help deter the radicalization process and help prevent the spread of violent extremism that leads to violence.

According to Zulli et al. (2021), public relations are at the forefront of research involving foreign terrorist threats and activity crises. However, in this case, little attention is given to domestic terrorism and violent extremism, leading to an increase in domestic terrorism in the United States. Zulli et al. suggest that 40 years of media coverage on domestic terrorism indicates four theoretical factors related to crisis management and issues involving domestic terrorism associated with the news media coverage related to “sourcing, contextualization, ideological labeling, and definitional uncertainty” (p. 1). Information suggests the four factors in how domestic terrorism is viewed today are related to:

1. Over the years, views on domestic terrorism have been contextualized and shifted.

2. Domestic terrorism groups and organizations' ideological labels apply to right-wing domestic terrorists rather than left-wing terrorism.
3. The definition of domestic terrorism has changed over time.
4. Future research should focus on gaps in research concerning "public relations and crisis management" (Zulli et al., 2021, p. 357).

Zulli et al. provided the example that occurred in October 2020, involving a domestic terrorist threat against the governor of Michigan, when "three right-wing extremists were arrested in a failed attempt to kidnap the governor" (p. 2). If there is no actual definition on how to handle or prosecute domestic terrorist cases, "debates underscore the constitutive yet contested nature of terror crises," and how domestic terrorism cases are defined is reliant on a clearer picture, "construction and management of terrorist crises" and who is defining the crisis (Zulli et al., 2021, p. 358). The Bible provides a clear picture of false prophets stating, "Beloved. believe not every spirit but try the spirit whether they are of God because many false prophets are gone out into the world" (*King James Bible*, 1769/2021, 1 John 4:1).

According to Chalk (2020), the relationship that countries such as the UK, France, Canada, and Australia have in addressing domestic terrorism is based on mitigating terrorist threats, the role law enforcement has in preventing domestic terrorism, and the mechanisms applied to review and control domestic terrorists and organizations. In the UK, the apparatus used to mitigate domestic and international terrorism involves several agencies that collect data and covert information to conduct a unified effort to address domestic and national threats. Chalk wrote to mitigate issues that are immediate and long-term threats related to domestic, the Joint Terrorism Analysis Centre (JTAC) manages terrorism threats, homeland security, and national security established in 2003. The primary goal is to synthesize data and information collected to analyze and assess threats identified by law enforcement agencies and HUMINT. The HUMINT efforts may involve community residents and law enforcement in collaborative efforts to target individuals, groups, and domestic terrorist organizations and their infrastructure, plans, and capabilities. Chalk (2020) noted around 2018, the French president created a “20-member National Centre for Counter-Terrorism” (p. 10) designated to monitor counterterrorism efforts and determine necessary strategies to mitigate risk, vulnerabilities, and threats. In Canada, counterterrorism efforts are the responsibility of the Canadian Security Intelligence Service (CSIS), an agency tasked with data and intelligence collection from principal resources such as “human intelligence (HUMINT), signal intelligence (SIGINT), and open-source intelligence (OSINT)” that may include video surveillance, intercepting communications, and cover-undercover operations (Chalk, 2020, p. 12). The CSIS is tasked with providing time-sensitive reports based on “threat assessments, and a strategic analysis on threat risk assessment” (Chalk, 2020, p. 13).

In 2019, the Canadian government passed Bill-59, legislation designed to provide a “higher degree of granularity for defining the powers and operational latitude granted to CSIS under the 2015 Act” (Chalk, 2020, p. 13). Bill-59 represents the importance of intelligence sharing between the community, law enforcement, and governmental departments. Chalk (2020) stipulated that the CSIS agencies cannot engage in actions involving torture and risk associated with endangering life and can impede travel and intercept communications. In addition, specific information can be held concerning retaining data sets, governing personal information, and tightening how terrorism is defined. A significant function of the National Security and Intelligence Review Agency (NSIRA) is to “create a super-watch dog” to coordinate counterterrorism actions and activities of CSIS, the CSE, and the Royal Canadian Mounted Police (RCMP), according to Chalk (p. 14).

According to the FBI, the "sovereign citizens" movement is considered to be a domestic threat in the United States, not a terrorist organization, but a "movement of loosely affiliated, similarly minded, individuals"(Sarteschi, 2020, p. 6). These groups are considered a threat in the United States because of behavior inconsistent with the rule of law and conduct, which threatens nonsovereign and law-abiding citizens. These individuals are considered dangerous and believe America is an illegitimate government with no absolute legal authority. The DHS (2021) has designated the "sovereign citizens as extremists" (p. 8) which can include individuals, groups, or organizations that commit acts of violence directed toward government officials and institutions and consist of government facilities. In this case, the term extremist is not used to define or identify sovereign individuals or groups. However, the term applies because they can engage in violent extremist acts of violence. Sarteschi further explained that sovereign citizens could be found on websites showing individuals interacting with government and public officials, arguing against various laws, and trying to "argue their way out of law violations" (p. 8). The psychological behavior of sovereign citizens is seen in the difference in belief systems, core beliefs, tactics, and how individuals display a sense of self-identity.

Rich (2020) explained that extremism has been around in the United States since the 19th century and is poorly framed in many people's minds in some parts of society. In later years there has been an increase in far-right extremist and domestic terrorism in crime dramas, westerns, and romantic melodramas. These factors are terrains for external terrorists outside the realm of Hollywood. For example, according to Rich, during the1990s, American cinema began depicting the Ku Klux Klan (KKK), skinhead extremists, neo-Nazi groups, and patriot militias.

Domestic threats have contributed to these groups to an increase in extremism. In later years, research studies have linked some far-right ideologies and the motives of jihadist terrorist groups and organizations to the radicalization process by instilling radical beliefs and jihadist ideologies in the minds of new members designed to target governments.

According to Rich (2021), in some parts of society, radical White supremacy movements express concerns about a range of issues and demonstrations that lead to perpetrated violence, a range of hate crimes, and violent extremist attacks. In addition, far-right domestic terrorism is often seen exerting support that “reinforced established patterns of racial and ethnic domination, often involving local law enforcement bodies” (Rich, 2021, p. 163). Between 1920 and 1979, the new left terrorism emerged and became more prominent and viewed from a strategic standpoint directed toward breaking opponents’ will and instilling fear and attainment to achieve a broader political objective to achieve power. According to Rich, far-left terrorism can elevate its terrorist tactics and strategies and support underground groups and movements that do not have links to political affiliation and support at the center of politics.

According to Tamborini et al. (2020), when there is news coverage of domestic terrorist events, this often increases “moral institution salience” (p. 511) and impacts the level of respect for government authority and law enforcement. An example is the media coverage and exposure to news concerning the terrorist attack in Paris, France, in 2015 and based on a sample of data collected from U.S. participants involving the domestic terrorist attack in the 2017 Las Vegas, Nevada music festival shooting. Tamborini et al. suggest even though the motive was unclear, the news coverage concerning the attack in Paris may have influenced the Las Vegas attack and had an overall impact on the audience's perception regarding the level of safety, cohesion, and “increased the salience of binding moral intuitions” (p. 551). Tamborini et al. suggested domestic terrorism and extremist violence increasingly expose victims, perpetrators, and other domestic terrorist actors to violent events and mass shootings that have a reminiscence of domestic and international terrorism. These events also inspire actors and perpetrators, increase the “salience of moral instincts,” and motivate other domestic terrorist actors (Tamborini et al., 2020, p. 512).

Tamborini et al. (2020) further explored moral instincts from a psychological and moral foundational and theoretical (MFT) perspective; defining the term as “bits of mental structure” that develop over time when an individual has been exposed to different events that “operate preconsciously to govern moral judgments” (p. 512), and thoughts that shape experiences. Based on exemplification theory and models of intuitive morality and exemplars (MIME), Tamborini et al. suggest continuous exposure to media coverage of domestic terrorism and violent extremism can have a long- and short-term impact. It can stimulate mental functions associated with moral intuitions and impact attitudes, decisions making, and the behaviors of domestic terrorists and extremists and have an impact on the minds of members of an audience, according to Tamborini et al. Research has shown five MFT intuitions that have an impact on individualized and binding moral institutions in the level of authority, loyalty, and participation in domestic terrorist groups and organizations, according to Tamborini et al. (p. 513).

Mahoney (2020) discussed nonstate extremist groups and organizations that issue bluffs and threats as a means to intimidate, coerce, and issue threats against civilian populations and governments to help strengthen the groups’ credibility. Bluffing is considered a common tactic used to achieve specific goals and help advance the groups’ strategic goals through methods designed to outbid rivals, interrupt the peace process, intimidate civilian populations, and promote violence and violent activity threats. Exploring motives behind bluffing suggests it is a tactic that provides incentives to nonstate extremist groups and provides strategic rationales that can include empty threats to pursue new objectives. Mahoney explained that assessing extremist terrorist bluffs will help determine if a group has the motivation and can help identify distinct campaigns and determine if bluffs contribute to advancing these specific objectives. In some cases, bluffs are used to threaten future violence against civilians and advance specific interests or objectives without violence or violent activities. When extremist groups use bluffs to terrorize civilians and governments, it is often to estimate the cost of damage, project its power, and the potential cost of future incidents. Mahoney further stated that when bluffs are used against citizens and government agencies, extremist groups and organizations attempt to raise awareness, publicize grievances, and coerce the government into compliance with their threats. Future research can focus on examining patterns in the behaviors of extremist groups and domestic terrorist groups to determine if specific bluffing patterns have been used to expand in geographical locations and regions. This focus may help understand the rationale behind the motives of extremist groups and organizations as well as understand the rationale behind the groups' target selection and enable researchers to test hypotheses related to empty threats, according to Mahoney.

Violent Extremism and Anarchists

A comparative study involving domestic terrorists identified as violent extremists suggests these groups are motivated by political and ideological goals and objectives. The radical group leaders are often male, older, and likely to be part of the ethnic majority (Jasko & LaFree, 2020). In the relationship between leader and follower, leaders are more committed to the organization's ideologies, goals, and objectives. Followers are more committed to committing and engaging in extremist acts of political violence to support the group's ideology, goals, and objectives. In recent years, extremist and radical groups have increased, and followers are expected to support the groups' or organizations' shared goals that may vary according to membership in the group and members' level of motivation, personal preferences, and knowledge (Jasko & LaFree, 2020).

In the United States, Jasko and LaFree's (2020) research suggests in domestic terrorist groups, a "third of the members classified as leaders and two-thirds are considered as followers" (p. 141), and there are differences in age, gender, minority status, and socioeconomic position. Members are committed to the mainstream goals and objectives of the organization and willing to commit political acts of violence. However, in multivariate models used to compare leaders' and followers' motivation for committing political violence, Jasko and LaFree noted a lack of research in these areas. Thus, research gaps exist, but research has shown differences in leader-follower characteristics, specialized knowledge, and incentives in the organizational structure. Still, followers must demonstrate a commitment to the group's and organization's ideology, cause, and potential psychological rewards for committing political acts of violence.

According to J. Bell (2019), the United States has a long history of race relations and far-right extremism. In the United States, White supremacy has been at the forefront of violent race-related activity. Around the country, they are responsible for many expressions of racism and racist violence. J. Bell pointed out that since the election of the first Black president, it created a postracial environment. Since the 2016 election, the country has seen an increase in the "number of documented race-based hate crimes" (J. Bell, 2019, p. 305) and crimes motivated by bias targeting different races. Since the 2016 election, there has also been an increase in violent extremism and "tenets of White supremacy" (J.Bell, 2019, p. 305). J. Bell noted that hate crimes and extremism blanket most of the country, with no sufficient remedy to stop hate crimes even though most hate crimes are prosecuted on the state level and not the federal level. Currently, five states do not have state laws or legislation concerning hate crimes, including Arkansas, Georgia, Indiana, South Carolina, and Wyoming (J.Bell, 2019, p. 305). Depending on the nature of a hate crime, some hate crimes are prosecuted on the federal level.

J. Bell (2019) suggested that in some cases, under the Hate Crime Statistics Act of 1990, law enforcement agencies are required to report hate crimes if the crime fits a specific pattern. A report by the Associated Press indicated that between 2009 and 2014, half of law enforcement agencies in jurisdictions in Indiana failed to report incidents involving hate crimes to the FBI (J. Bell, 2019, p. 313). In 2016, according to J. Bell, the FBI suggests some law enforcement agencies in Indiana claimed there were no hate crimes committed in their jurisdiction. J. Bell further explained that in states that do not have hate crime laws, a cross burning is considered a “simple trespass case” (p. 314), and these weaknesses in some institutions contribute to an environment that supports hate crimes and creates barriers that make it hard to address the dangers posed by violent extremists.

According to Saito (2019), in a 2017 report, the FBI Counterintelligence Division suggests groups identified as Black identity extremist (BIE) groups were motivated by the unfair treatment of African Americans and actions designed to perpetrate violent acts against law enforcement and communities. Saito pointed out that the BIEs threat is no comparison to White supremacists, and members of BIE groups attempt to identify with the BLM group to perpetuate dangerous, violent extremist actions often seen in acts of violence during peaceful demonstrations with other extremist groups. The 2017 FBI report indicated that BIE groups have been responsible for an “increase in premeditated, lethal retaliatory violence against law enforcement” (Saito, 2019, p. 4). In a volatile environment, BIE groups are responsible for perpetrating violence against law enforcement and use police brutality as a reason for "justification for such violence in the future" as a retaliatory measure (Saito, 2019, p. 4). However, Saito noted that left-winged extremism often involves private acts of violence perpetrated by anarchists and Black nationalists. Evidence does not suggest these extremists are a threat to law enforcement, and right-wing extremism poses a more significant threat because of the evidence of racism and the level of violence. Saito further explained that self-styled liberals and progressives claim nationalism fosters radicalization elements and radicalizes hatred, which risks public safety.

According to Ganesh and Bright (2020), anarchists and extremists have exploited the internet and social media platforms with propaganda, impacting how some civil societies, governments, and the private sector function and raising concerns for counterterrorism experts. Ganesh and Bright explained that the internet and social media are vehicles used to spread hate narratives, promote propaganda activities to solicit terrorist financing, and radicalize members. Mitigating violent extremism requires a counterterrorism strategy designed to counter violent extremism; therefore, countermeasures should include a strategic communication plan targeting violent extremism and preventing extremists from exploiting social media platforms. Ganesh and Bright stressed that future research on mitigating domestic terrorism and extremism must take a multistakeholder approach to challenge the violent extremists' ability to influence the internet and social media and use these resources as a platform to spread violent extremism. Many open democratic societies should examine how to prevent the "exploitation of social media platforms and is an essential regulatory question for civil society, government, and the private sector" (Ganesh & Bright, 2020, p. 7). Future research should be conducted to examine social media outlets when bluffs made by domestic terrorist groups as threats made through social media, this will help analysts determine empirically if bluffs are empty threats and test any hypothesis using data-based tools to evaluate these problems.

Counterterrorism

Weeks (2019) stated that in counterterrorism, radicalization and political violence are a concern, and it is a social problem in society that requires measures to mitigate extremism and threats. He recognized radicalization theories coalesce around factors such as identity, grievances, or foreign policy elements and support for ideologies, and radicalization is a process like a conveyer belt theory that involves a series of progressive steps (Weeks, 2019). As an individual becomes more radicalized, the process leads closer to violent behavior. To combat the radicalization process will require assessing the "mainstream political thought in a given period" (Weeks, 2019, p. 741).

According to McIlhatton et al. (2020), in a quantitative research study on counterterrorism that involved a methodological framework including structured interviews conducted in local and international jurisdictions in the United Kingdom, United States, and Australia to conduct risk assessments on critical infrastructures and core features of development projects, the goal was to protect against acts of terrorism (p. 753). The research study focused on two inquiries associated with understanding the importance of counterterrorism in the real estate development process and assessing the counterterrorism barriers in providing protective security in large venues where crowds gather for specific events or functions. McIlhatton et al. suggested in the research literature on elements of counterterrorism, the focus is placed generally on measures needed to mitigate threats through policies and strategies aimed at mitigating the threat, removal of the threat environment, and individuals, groups, and organizations that are a threat to homeland security and national security. However, there is a limited body of work on anti-counterterrorism measures.

These measures are designed to provide a defensive posture to protect and prevent acts of terrorism, especially in environments where there is an increase in crowds, an attractive backdrop to terrorists. However, in counterterrorism, some barriers inhibit counterterrorism measures and protective strategies in some future development projects. Therefore, McIlhatton et al. (2020) suggested in counterterrorism to reduce elements of terrorism, counterterrorism and antiterrorism are measures designed to take into consideration three approaches

1. Counterterrorism measures can include mitigation to remove the threat environment, individuals, groups, and organizations.
2. Counterterrorism measures can include deploying “hard-line and soft-line measures” in response efforts.
3. Anti-terrorism measures can include measures commonly used in the United Kingdom’s design to provide protective security (McIlhatton et al., 2020, pp. 753–754).

McIlhatton et al. noted that in counterterrorism, there is little research literature and a reduced knowledge base on these anti-terrorism measures that can include taking action to mitigate terrorism and how to, protect crowded places, and protecting cities from the threats, risks, harm, and acts of terrorism. A significant attractor to terrorists in modern society is events that accommodate large crowds, such as concerts and sporting events. These venues require counterterrorism measures designed as proactive security for events requiring planning, defensive, and crowd control measures. McIlhatton et al. suggested future counterterrorism research should explore gaps in research associated with an integrated security management system, and special consideration should be given to real estate developments that accommodate large crowds and ensure personnel is well-trained, educated, vetted, and policies and procedures around other security-related issues that are not always present. McIlhatton et al. feel defensive measures are not limited to methods in physical and proactive security measures.

According to Tung (2019), mitigating domestic terrorism and violent extremism in the United States requires counterterrorism strategies and information operations designed to meet three strategic goals and objectives:

1. Intercept domestic terrorist groups and extremist communications to determine the adversary's plans.
2. Obtain information through surveillance, wiretaps, and warrants on domestic terrorist groups and extremists to determine intentions, locations, objectives, and goals.
3. Once critical information has been obtained, implement necessary measures, disrupting a planned attack, disrupting those potential attacks, and capturing domestic terrorists (Tung, 2019, p. 560).

In counterterrorism, detection is an essential part of mitigating threats. Passive detection measures can provide background sounds such as television and radio transmissions to determine the potential location (Tung, 2019). In the United States, fusion centers are another counterterrorism tool in counterterrorism operations used to collect data, information, and surveillance from other federal and local law enforcement agencies on domestic terrorists and violent extremists.

According to Nguyen (2019), law enforcement has a critical role in counterterrorism efforts in preventing domestic terrorism across the country. Domestic terrorism has become an immediate homeland security and national security concern. Measures taken to combat domestic terrorism are also a concern for citizens due to a fear of a potential erosion of civil liberties and other constitutional rights. As a result, some law enforcement agencies have adopted measures and programs like “countering violent extremism (CVE) initiatives,” according to Nguyen (p. 322). These programs are a driver of programs directed toward mobilizing communities and developing a strategic community strategy to mitigate homegrown terrorism and other forms of domestic terrorism such as street gangs, lone-wolves, White supremacists, and militia groups. The DHS supports change drivers through federal government grant programs to local law enforcement and designated community groups.

Schuurman et al. (2019) suggested that the lone-wolf concept has a different typology from a violent extremist in the counterterrorism profession. Empirical research suggests that online and offline activities are critical to how these terrorists adapt to radical terrorist behavior and are motivated to commit violent acts of terrorism. Regarding the pre-attack actions of the lone-wolf type, these individuals “are not stealthy and highly capable” of committing acts of terrorism (Schuurman et al., 2019, p. 771). In research findings, the lone-wolf concept should be redefined to prevent closing off the ability for detection and interdiction in counterterrorism. On the other hand, lone actor extremists in the United States are currently on the rise, and the perception of lone-wolf terrorists has been misconceived and questionable. This calls into question the ability to detect, prevent, and respond to these types of threats.

In some cases, these types of terrorists are motivated by interpersonal, political, and ideological viewpoints, have ties to other operational features, and are connected to more extensive networks. Schuurman et al. (2019) suggested how lone-wolf extremists are defined and should be overhauled but should be considered single operatives with a mission to conduct or carry out a specific threat. Law enforcement and intelligence agencies must engage in early detection methods to prevent attacks and deploy countermeasures in counterterrorism. Schuurman et al. further suggest it is essential for counterterrorism professionals and law enforcement to understand that among lone-wolf extremists, loneness, social isolation, and poor social skills are traits of these individuals. Some of these individuals are psychologically triggered by personal motivation and a commitment to support causes led by potential co-conspirators (Shuurman et al., 2019).

According to Boukalas (2019), in the United Kingdom, counterterrorism policies are directed toward mitigating counter-extremism. Boukalas noted that counter-extremism programs are designed to avert the potential of government failure and divides in society along political lines or create a culture that mobilizes security in all parts of society. In the United Kingdom, counter-extremism is prominent in institutions, and strategic planning helps to secure many aspects of society from extremist activity (Boukalas, 2019). The prevention strategy serves as an intervention in the community, state, and intercommunity relations designed to improve counterterrorism efforts through collaborations and cooperation from diverse and multicultural communities (Boukalas, 2019). Counter-extremism involves the whole society, and the state is responsible for deciphering key element and their implications. Therefore, preventive programs help the state counter the threat of extremism. The prevention paradox is an antiliberal position to secure and perpetuate liberalism to take a different approach to extremism without violating civil liberties and other freedoms, according to Boukalas.

To mitigate threats related to terrorism, Milton and Price (2020) noted that leadership decapitation is a method used to remove the leadership of terrorist groups and organizations. Research suggests what complicates matters in this approach is the longevity in external relationships and conditions that can impact elements of leadership. Milton and Price suggested some literature on terrorist networks, and leadership decapitation supports the notion that some terrorist organizations, networks, and operational functions can be impacted if there is leadership decapitation. Many terrorist groups and organizations are susceptible and vulnerable to leadership decapitation. When these counterterrorism tactics and measures are used to address leadership in terrorist groups and organizations, the literature suggests the following:

1. Leadership decapitation can impact the organization's performance, longevity, and ability to function and plan activities.
2. Based on research literature, there is an argument suggesting "highly networked terrorist groups and organizations tend to be more resilient to decapitation," and other members can assume the leadership role (Milton & Price, 2020, p. 310).

Milton and Price delineated that leadership decapitation and terrorist networks are two different research topics. In many cases, terrorist groups and organizations attempt to avoid actions that create vulnerabilities and are vulnerable to a state's counterterrorism apparatus, measures, and tactics.

Future research should examine gaps in research associated with leadership in domestic and international terrorist groups and organizations impacted by leadership decapitation and the ability of these organizations to plan, function, and operationalize. Future research should also explore how "small-scale connections can lead to leadership and management" changes in these organizations (Milton & Price, 2020, p. 320). To root out threats to the homeland and national security requires a framework that examines different perspectives.

Protecting Critical Infrastructure and Key Resources

According to Sauter (2020), in 1977, the Department of Energy Organization Act established the Department of Energy (DOE), which serves as a cabinet-level agency tasked with oversight and monitoring America’s agencies that provide nuclear power and energy programs (p. 6). These measures also include guidance and recommendations on securing and protecting nuclear and energy infrastructure sectors from cyber threats and malicious cyber-attacks. Sauter explained that the DOE is designated as the “lead sector-specific agency for cyber-security” (p. 6) and collaborates with partners and stakeholders to ensure the nuclear and energy sector infrastructures are protected from cyber threats that can impact systems networks and operational functions. Under the DOE, the agency established the cybersecurity capability maturity model (C2M2) in a multiyear program designed to help secure facilities, evaluate processes, identify and prioritize vulnerabilities, and help improve cybersecurity measures for nuclear facilities, oil, electrical power grid systems, natural gas facilities, and pipelines (Sauter, 2020, p. 6).

In 1990, experts warned that the U.S. energy sector was susceptible to cyber-attacks, and a small number of cyber-attackers could cause significant disruptions to the nation’s electrical grid system. According to Sauter (2020), in 2017, U.S. energy companies were compromised and targeted by “Russian advanced persistent threat actors” (p. 5) that obtained control over an electrical grid system causing massive blackouts, and in 2018, another cyber-attack led to multiple pipeline failures in natural gas pipeline communication systems.

Additionally, Sauter (2020) described a cyber-attack that targeted a natural gas compression facility and impacted natural gas distribution for several days. Experts feel a more targeted cyber-attack could potentially impact natural gas transmission, distribution, and interconnectivity and force an operational shutdown geographically. As a result, cyber-threats in the U.S. energy sector are among the greatest threats to critical infrastructure that can cause massive disruptions in major cities and rural and metropolitan areas. According to the Pipeline Cybersecurity Initiative Fact Sheet, Sauter further noted that the Cybersecurity and Infrastructure

Security Agency (CISA) provides stakeholders, owners, and operators with guidance based on three assessment types that also examine probabilities (p. 520). The assessments include the following:

1. Tier-I assessment involves a multiday assessment for conducting an evaluation.
2. Tier-II assessments involve the ability to conduct a single-day assessment for evaluation.
3. Owners and operators use Tier-III assessment to conduct assessments independently (p. 520).

Under the U.S. Government Accountability Office, GAO-19-426, a critical infrastructure pipeline is required to complete security documentation related to essential infrastructure operational functions and the environment (Sauter, 2020).

According to Wei et al. (2020), to manage critical infrastructure, there must be a support system that assists in providing guidance and recommendations "for urban infrastructure inter-asset management" of critical infrastructure (p. 2). These vital infrastructures can include rural and urban street works, including roads, bridges, pavement maintenance, water distribution systems, natural gas distribution, and natural gas transmission pipelines. Therefore, leaders must be familiar with these challenges and infrastructure management systems and manage critical infrastructures in multiple leadership roles (Wei et al., 2020). For example, the first challenge is working interdependently on numerous groups when critical infrastructures involve underground utilities. The deterioration in concrete and pavement can impact roads and streets and cause significant damage to assets such as underground electrical and communication cables, water distribution systems, and natural resources gas pipes. The second challenge is "urban infrastructure management" systems that require leaders to compile data from several sources and can include data from engineers, such as "underground utility maps, road construction details, and road closure regulations" (Wei et al., 2020, p. 2) and is located where specific utilities are buried underground, which in many cases will require data from a utility locator.

The third challenge can include mitigation to schedule timely or routine maintenance that is proactive and allows leaders to "predict the potential consequences of actions and observations in infrastructure management to apply appropriate countermeasures" (Wei et al., 2020, p. 2). Mitigation includes necessary measures to identify hazards, risks, vulnerabilities, and threats that can impact society if there are failures, distribution problems, and domestic terrorist incidents. The goal is to determine if there are any environmental concerns, such as risk and vulnerabilities and the potential for contamination, traffic delays, and disruption, and identify behavioral concerns that can impact operational functions. Many critical infrastructures require technology, system networks, and communication technology to perform well to maintain the continuity needed for operational processes to deliver resources. Wei et al. (2020) also explained that critical infrastructures require "intelligent web-based decision support systems" (p. 2) for infrastructure management system-of-systems to support different operational functions. These systems are used to manage underground conditions or "Assessing the Underworld DSS, referred to as ATU-DSS," which deals with roads, pavement, underground utilities, and surface conditions that impact underground utilities (Wei et al., 2020, p. 2). These systems use a set of building blocks that trigger in the event of abnormalities and anomalies in data inconsistent with current and historical data and based on a "rule-based and real-time data" approach developed by domain experts, according to Wei et al. (p. 2). In addition, Wei et al. recommended that future research on critical infrastructure explore measuring uncertainty by applying quantitative metrics and "qualitative linguistic expressions," a method based on human reasoning to assess and determine “a qualitative confidence levels-based uncertainty management scheme” used by domain experts to compare linguistic qualifiers based on “fuzzy sets theory” (p. 6).

According to Luskova and Dvorak (2019), critical infrastructures and key resources are considered an asset or system that provides needed resources where any disruption or destruction can have an enormous impact on how the economy performs as well as the social fabric of many communities. Luskova and Dvorak noted these resources are vital to the quality of life for people living in a community that relies on specific resources to protect “life, health, security, property, and the environment” (p. 7). These resources include the local food chain, water treatment facilities, hospitals, banks, social services, police and fire, electrical grids, and natural gas pipelines. In addition, Luskova and Dvorak explained that protecting critical infrastructures requires conducting a risk assessment to determine vulnerabilities. A risk assessment is a functional plan of action designed to provide a framework and application in a risk management plan and security plan to protect critical infrastructure and key resources, including security measures for detection to prevent disruptions and the destruction of elements of critical infrastructures. Critical infrastructures and key resources include both public and private entities. As Luskova and Dvorak noted, ensuring the protection of these infrastructures requires cooperation from the public and owners/operators of infrastructures in a proactive approach to secure critical infrastructure.

According to the Interstate Natural Gas Association of America (INGAA) and the American Petroleum Institute (API), the Protecting Our Infrastructure of Pipelines and Enhancing Safety (PIPES) Act of 2020 received high praise from the INGAA and API (“INGAA, API Laud Congressional Passage of PIPES Act,” 2020, p. 53). The new legislation is part of the 2020 omnibus spending bill, and the goal of the bill was to provide guidance and enhance safety for workers and strengthen and enhance safety protocols under the Pipeline and Hazardous Materials Safety Administration (PHMSA; "INGAA, API Laud," 2020, p. 53). In addition, the PIPES Act aims to enhance measures for public safety and protect the environment and includes the following requirements:

1. PHMSA must provide safety measures designed to detect leaks and new regulations for repairing and class location and enhancing public safety measures.
2. PHMSA will provide additional funding for pipeline safety at the federal and state levels.
3. PHMSA requires operators to modernize and upgrade facilities and safety regulations for LNG export facilities.
4. PHMSA requires operators to enhance safety measures and public safety in local distribution systems.
5. The new grant system under PHMSA will provide "emergency responders, public safety, advocates and community groups" ("INGAA, API Laud," 2020, p. 53).

The PIPES Act also includes additional measures to ensure "improvements in environmental performance" ("INGAA, API Laud," 2020, p. 53) and ensure processes contribute to reducing emissions.

In the United States and countries such as the United Kingdom, there are "sprawling networks of natural gas infrastructure" (Forman, 2020, p. 143) as well as landscapes that are constantly changing and require security measures designed to protect and mitigate dangers associated with the flow of underground natural gas. For example, in the United Kingdom, the National Transmission System (NTS) consists of natural gas transmission pipes that are "7,600-km-long and 280,000 km of buried distribution pipes" (Forman, 2020, p. 143), which is part of the National Grid System (NGS). According to Forman (2020), the NTS monitors the distribution and transmission of high volumes and high-pressure natural gas from producers and international connections and involves networks that distribute natural gas on a regional scale. In subterranean infrastructures involving natural gas in the United Kingdom, there are dynamic fields of risk broken down for two reasons: (a) ensuring natural gas pipelines are a distance from actors that can cause disruptions and gas to escape; and (b) making circulatory infrastructures remain unknown to actors, minimizing the risk of interference or domestic terrorist incidents.

In natural gas production, transmission and distribution are the primary functions in the high-pressure transportation of natural gas (Quinn, 2020). Transmitting and transporting natural gas through a maze of pipe systems requires forecasting an adequate amount of pressure. Therefore, forecasting rooms must have “natural gas pipeline pressure alarms” (Quinn, 2020, p. i) and sensors that allow operators to maintain gas line pressure. In natural gas production, safety is another primary concern, and many pipeline failures occur due to natural gas pipeline infrastructures that become old over time and are not adequately maintained. According to Quinn (2020), the PHMSA is currently responsible for enforcing federal regulations and industry standards, including ensuring operators use the latest safety technology to protect critical pipeline infrastructures and production and support public safety. Natural gas transmission and distribution also have negative environmental impacts and safety concerns. However, natural gas transmission is considered the “cleanest burning fossil fuel and energy-efficient and most cost-effective way to deliver, distribute, and transmit natural gas over long distances” (Quinn, 2020, p. 27). Therefore, in the production and transmission of natural gas, sensors and digital technology play a critical role in maintaining, controlling, and protecting pipeline infrastructure in ensuring more competent and smarter production and can contribute to a higher volume of natural gas with fewer errors and care to the environment and public safety (Quinn, 2020).

According to DiChristopher (2020), high-level concerns were expressed about the risk associated with state-sponsored hackers in natural gas production and distribution. Cyber-criminals continuously attempt to penetrate operational functions in industrial control systems in facilities that house electrical grid system controls for utilities, refineries, oil, and natural gas pipelines (DiChristopher, 2020, p. 1). Companies that fail to follow the DHS cybersecurity and infrastructure security protocols run the risk of failure in the organization's information technology (IT) segment. As DiChristopher explained, in the production, distribution, and transmission of natural gas, a cyber-attack has been a long-standing concern for some facilities with inadequate IT security for natural gas compression. An alert issued by the DHS in February 2020 revealed an unnamed natural gas facility was targeted and susceptible to hackers gaining access to the IT systems (DiChristopher, 2020, p. 1). Information system technologies infected with ransomware could penetrate operational technology and systems networks, which can impact control and operational functions. The cybersecurity contractor Dragos issued a statement that suggests the cyber-attack “did not attempt to intentionally alter, modify, and degrade the integrity of industrial control systems at the gas compression plant” (DiChristopher, 2020, p. 1). A significant factor related to the cyber-incident was partly due to a failure to install security barriers between IT and operational technology (OT) systems, according to DiChristopher. The DHS alert highlights the importance of information sharing among critical infrastructure in the energy sectors to mitigate cybersecurity threats and physical threats to critical infrastructures and key resources facilities in real-time and monitored IT systems 24 hours a day by experienced IT technicians.

According to Uberti and Stupp (2021), the recent Colonial Pipeline hack in May 2021 illustrates the need for a regulatory body to enforce cybersecurity standards for oil and gas producers. In this case, the hacking attack on one of the nation's most significant oil, fuel, and gas producers had a catastrophic impact, causing substantial shortages in fuel supply and a considerable increase in fuel cost. The magnitude of the Colonial Pipeline shut-down extended to "5,500-miles of pipelines and stretches across the Gulf Coast to New Jersey" (Uberti & Stupp, 2021, p. 2). In addition, Uberti & Stupp noted in a 2019 report issued by the GAO cited that hackers could target the pipeline information technologies. The pipeline security had vulnerabilities that extended to staff shortages, and the company lacked cybersecurity expertise. Therefore, businesses in the energy sector must take cybersecurity more seriously and obtain the necessary resources to mitigate hacking, cyber-criminals, and ransomware.

According to Good (2020), suggest in the past, oil and gas pipeline companies were warned that cyber-attacks could have a significant impact on mainstream businesses and natural gas compression facilities and could negatively impact the credit rating of companies. When electrical power grid systems or oil and natural gas production IT are affected by ransomware, credit ratings are impacted, and utilities are at risk. Good suggests owners and operators of these infrastructures are responsible for preventing cyber-attacks and must mitigate "front-office operations such as email and internet activity from cyber and physical threats that can impact "operation technology systems, and industrial control systems" (p. 1) from cyber threats, hackers, and other cyber-risks. The DHS suggests in the event of an intrusion, employees must be trained in emergency response, address cyber-risk and threats, and have decision-making skills to mitigate cyber-threats.

On May 27, 2021, the DHS issued the first cybersecurity guidelines, requirements, and regulations for operators and owners of critical oil and electrical power grid systems and natural gas pipelines. The new security directive falls under the purview of the Transportation Security Administration (TSA). The goal is to ensure essential infrastructure has the capabilities and capacity to mitigate hackers and cyber-criminals and prevent cyber-threats from threatening the stability of critical infrastructures that provide necessary resources such as electricity, oil, and natural gas to pipeline sectors. The new requirements are due to the ransomware attack on one of the nation's largest petroleum pipelines and producers and growing concerns that hackers or state-sponsored terrorists can hack into another oil and natural gas or electric power grid system critical infrastructure.

The DHS collaborates with partners to help create resiliency in technology and controls in information technology and operational functions to help prevent cyber-attacks. For example, the cyber-breach and attack on the Colonial Pipeline operational controls demonstrate the need for more resilient and robust cybersecurity. The federal government is working closely to monitor private partners to ensure adequate cybersecurity. Under new DHS requirements, owners and operators are required to report cyber-incidents to the "DHS Cybersecurity and Infrastructure Security Agency (CISA) and the designated cybersecurity coordinator within 24 hours and seven days a week" (p. 1). DHS initiatives also require owners and operators to assess gaps in cybersecurity and mitigate any problem identified during risk assessments which must also be "reported to TSA and CISA within 30 days" (p. 1). The new requirements also highlight the TSA's role in strengthening cybersecurity to ensure that electric power grid systems and oil and natural gas pipelines are secure and resilient, and measures to mitigate ransomware, cyber-criminal, physical, and cyber-threats, according to DHS.

Schlette et al. (2021) explained that in cybersecurity, the primary purpose of cyber threat intelligence (CTI) is to contribute to data and information gathered on cyber threats and significant problems that can have an impact on other oil and natural gas pipelines (p. 21). CTI provides a platform that offers a means to share, detect, and protect against any potential cyber-threats that have been identified through CTI analysis and assessment tools designed to provide a "quality transparent assessment security" analysis of information technology (Schlette et al., 2021, p. 21) and operational technology systems on attacks and incidents that have occurred during operational functions. Empirical studies have shown leaders should collaborate with domain experts to understand the threat landscape and the benefits of sharing data and information to avoid operating under "inaccurate and incomplete data, or outdated threat intelligence" and risk assessments (Schlette et al., 2021, p. 21). The objective is to help prevent technical errors and inform other leaders, owners, and operators. CTI artifacts can assist analysts in understanding the nature of cyber threats and provide intelligence on threats that were identified and not known and require immediate attention to mitigate threats.

Christian (2020) noted in January 2020, Congress passed a new infrastructure framework design to provide support investments for electrical grid modernization systems and clean energy and address the most significant critical infrastructures and critical resources in the country. Funding allocation will include the following, according to Christian:

1. $1.5 billion in funding to replace aging natural gas infrastructures in some communities.
2. $2.25 billion in energy and solar grants and funding for low-income and underserved communities to replace outdated gas pipes.

3. $1.5 billion in financing for electric vehicles and charging stations to help reduce emissions (p. 1).
4. Funding for energy efficiency retrofits for homes and schools and supports weatherization programs in low-income communities.

Christian further explained that the overall framework is to help improve resiliency in critical infrastructure and key resources and protect communities in floodplain areas, such as funding energy efficiency programs, conservation programs, and intelligent technologies. In addition, the goal is to invest in underserved communities in need of critical resources to meet basic human needs, roads, and bridges, and support public safety. Today, members of Congress on both sides of the aisle are currently having debates on funding initiatives and the status of current critical infrastructures.

According to Hurdle-Lightfoot (2020), in natural gas production, distribution risk management is a significant function, and owners and operators of natural gas facilities and pipelines must maintain specific criteria and a current risk assessment plan. In natural gas pipeline production, industry owners and operators must develop an adequate risk assessment plan that focuses on safety. Companies should have the latest technology to monitor leaks and provide real-time condition reports on safety precautions necessary to maintain industry and policy standards systemwide. In the United States, hundreds of miles of natural gas pipelines exist. Therefore, leaders in homeland security and industry-wide must understand the benefits of effective risk assessment planning and update plans to address today’s challenges, problems, and changes in environmental conditions that can impact subterranean natural gas transmission lines and underground natural gas distribution pipelines to consumers. A similar risk assessment plan is expected for the electric power grid system, which must maintain continuity plans and have redundancy in its operational functions to provide service during power outages, downlines, and problems related to data breaches and operational functions.

Hurdle-Lightfoot (2020) noted an adequate risk assessment plans would help reduce profit losses, help maintain industry standards and maintain adequate safety plans and mitigations. In America, natural gas pipelines are one of the primary energy resources and are second to electrical power grid systems around the country. Natural gas pipeline upgrades and new community development increase consumption and the cost of gas to consumers and commercial customers. The natural gas industry safety initiative must include response plans, risk assessments, and assessing risks and vulnerabilities from production to distribution, operations, and servicing pipelines in fieldwork. A lack of these processes can have an impact on the industry nationwide and consumers. In the natural gas industry, the Occupational Safety and Health Administration (OSHA) Act of 1970 requires the industry to provide employees and organizational structures with safe working conditions and training on “how to maintain safety, risk assumptions, pre-job briefings, OSHA requirements, and emergency response protocols” (Hurdle-Lightfoot, 2020, p. 2).

In a quantitative research study on the nature of risk perception, the research should focus on the social reality, risk planning, and decisions made on housing projects and urban development where electric power grid systems and natural gas transmission pipelines are often related to land use and hazardous conditions. According to Hayes et al. (2021), in planning hazardous infrastructures, a view of land use requires assessing different degrees of risk, input from multiple stakeholders, and pipeline sector engineers’ assistance. The type of land use is an essential aspect of natural gas pipelines, and in urban development, careful consideration should be given to “high-pressure gas pipelines infrastructure” because third-party activity and excavations can have a devasting impact on communities in the near vicinity, cause dangerous fires and have an impact on public safety (Hayes et al., 2021, p. 183). Hayes et al. noted countries such as Australia, a “comparative analysis can be useful to highlight specific risk” (p. 183) and help determine the level of risk associated with new housing projects near a natural gas pipeline. Hayes et al. further noted there is evidence of broader risk in communities with hazardous infrastructures such as natural gas pipelines and electric power grid systems. Some political and institutional structures fail to understand fewer conflicts between people and community stakeholders, such as utilities in communities better serve public safety. Planning requires understanding elements of hazard creep, and new development projects in a community can impact existing hazardous pipeline facilities.

Advanced technology plays an essential role in public safety in critical infrastructures in communities, oil production, natural gas pipelines, and electrical power grid systems. Public safety relies on pipeline facilities and utilities to function efficiently in risk management and housing near schools and hospitals. Public safety in land use planning plays an essential part in the process and ensures the public domain remains safe. Risk governance is an integral part of planning to ensure all measures are taken to protect the public and the environment, including other critical infrastructures such as bridges, dams, roadways, and waterways. In some cases, where there is “hazard, creep associated with new residential development” (Hayes et al., 2021, p. 185), people living in the community development can be impacted by an existing high-pressure natural gas pipeline. A worst-case scenario is when a new development is in proximity to a high-pressure natural gas pipeline line. A lack of consultation with engineering experts can place communities at risk. Hazard creep can expose communities to hazards and consequences associated with a pipeline failure; if this occurs, relevant legislation will require modification to the pipeline system to protect the public domain and to reduce risk “as low as is reasonably practicable” (ALARP; Hayes et al., 2021, p. 184). According to Hayes et al., efforts will be required in collaborations between “planners, developers, regulators, and pipeline engineers” to review public risk factors (p. 184). In future land use cases and when natural gas pipelines are a development for the state, there must be a statutory policy for easements specific to be spelled out on a land title and physically marked on the property as a warning or to prevent incursions. Hayes et al. further noted in one case study within a multi-case study, in “Victoria and South Australia, to make a comparison between governance frameworks and risk perceptions” (p. 187), an evaluation was needed to determine the overall benefits of land use, including elements of planning and pipeline legislation that govern specific pipelines and key stakeholders (Hayes et al., 2021, p. 187).

In many parts of the country, oil and natural gas pipelines are susceptible to lightning strikes, and there are at least “2 million miles of oil and natural gas pipelines in North America” (Bickham, 2021, p. 32). Bickham (2021) also explained that lightning strikes in the environment are not the concern; the concern is the impact lightning storms can have on pipelines and controls systems, the lining of underground pipelines, and damage to coatings and cathodic protection (CP) systems used to monitor the conditions of underground pipes. Lighting strikes are different geographically, such as in the state of Texas, where systems are used to evaluate and monitor pipelines remotely. However, technicians must still perform inspections to assess the health of underground pipes and determine how systems are performing. When lightning strikes, it is hard to determine when a failure will occur, the extent of the corrosion, and how much downtime is required after a system failure. CP is a method used to assess and evaluate “different parts of a pipeline and pipe flanges" that have been directly hit by a lightning strike (Bickham, 2021, p. 32).

Brenna et al. (2020) explained that measures include efforts designed to cover different parts of the pipeline to protect oil and natural gas pipelines. One method used is CP, which refers to preventive measures designed to protect underground carbon steel pipelines from corrosion. It is a process "achieved by using a cathodic polarization below the protection potential, namely 0.85 V vs. CSE [CSE, copper-copper sulfate reference electrode] for carbon steel in aerated soil" (Brenna et al., 2020, p. 1). The purpose of the process is to prevent corrosion that contributes to corrosive effect throughout the thickness of the pipeline where alternating current (AC) and voltage can contribute to severe corrosion at "industrial frequencies between 50 or 60 Hz and when there are frequencies at 150 Hz, or higher the process decreases" (Brenna et al., 2020, p. 5). Therefore, factoring in AC density in preventing pipeline corrosion is significant in preventing and reducing erosion, causing a coating defect in the pipeline system.

Taquechel and Saitgalina (2018) stated to protect natural gas critical infrastructures, "risk-based performance metrics, and performance evaluation frameworks" (p. 2) are an integral part of the process. The homeland security and counterterrorism mission framework provide performance metrics as a critical tool to deter or prevent acts of terrorism and support anti-terrorism efforts. In elements of government performance metrics, Taquechel and Saitgalina note it is essential for government, especially in cases where measures are applied in government to help improve emergency outcomes and "public management and program outcomes" (p. 2). In homeland security, performance measurements and risk management help deter terrorism and acts of terrorism and reduce the potential consequences. In this case, the purpose of PRAs is to assess the likelihood and consequences of a pending terrorist attack involving critical infrastructures.

According to McCreight (2019), in managing critical infrastructures, vulnerabilities also extend to when an infrastructure experiences unforeseen incidents such as an electrical grid collapse, impacted by severe storm weather and wind conditions, “terrorism, technological accidents, cyber-attacks or geomagnetic storms” (p. 1). In the United States, from the perspective of homeland security, emergency management, and national security, there are three critical infrastructures, including “nuclear power plants, chemical manufacturing, and natural gas pipelines,” that have strategic significance (p. 1). As McCreight explained, if any of these energy systems and sectors experience significant disruptions or potential terrorist attacks at the operational level, this can have a cascading and devasting effect. Managing critical infrastructures requires leaders to ensure systems perform at an optimal level, and leaders must “mitigate loss, disruptions, discontinuity, and nullification of ordinary everyday services” (McCreight, 2019, p. 2).

According to Tata and DeCotis (2019), there are risks and vulnerabilities in delivery systems related to oil and natural gas pipeline production and electric power grid transmission. In the United States, a key driver of natural gas production is demand, and “inter- and intra-state pipeline projects” are constructed as infrastructure upgrade projects to meet the demands of existing customers and new communities (Tata & DeCotis, 2019, p. 1). In the production of natural gas, there are risk categories and high-level mitigation procedures. According to Tata and DeCotis, even though there are eight risk categories and vulnerabilities, the significant problems and risks are associated with the following:

1. Safety: Problems due to system failures and pipeline incidents causing injuries to workers, the public, and property damage.
2. Reliability: Problems related to “failures and damage to infrastructure and upstream supply constraints” (p. 8).
3. Execution: Problems related to weather problems, forced events, and problems due to strikes and protests.
4. Technical: Problems occur when pipelines require rerouting, "complexities in design,” and a lack of skilled workers (p. 8).
5. Financial: Problems are often related to cost overruns and materials, and sometimes upgrade projects lead to high restoration and upgrade costs.

Tata and DeCotis further noted between 2008 to 2018, there was a “total of 1,530 incidents across an average of more than 1.5 million miles of onshore transmission and distribution pipelines” (p. 4). Many of the incidents were material-related, pipe corrosion, equipment failure, and some underground pipe welds failed. Tata and DeCotis explained that condition monitoring is necessary to assess and monitor risk and pipes leaking, and mitigating risk requires monitoring pipe pressure and “reductions in operating pressures and scheduled repairs and replacements” (p. 4). There is a significant concern for natural gas producers in the aging pipeline infrastructure in many parts of the country. Among pipelines in service today, there are “1.6 million miles of the natural gas pipeline where approximately 48 percent were installed between 1940 and 1979, and 65 percent are natural gas transmission lines, and 35 percent are natural gas distribution” lines (Tata & DeCotis, 2019, p. 4). Another problem is that in some instances aging natural gas pipelines did not have installation or construction dates or data and information on when pipes were installed underground.

Under the DHS (2021b), the 2012 NIPP framework was designed to ensure the protection of critical infrastructures and key resources by providing guidance and recommendations on securing these CIKRs (DHS, 2021b, p. 1). In the United States, infrastructures are essential to national security, “public health and safety, economic vitality, and way of life” (DHS, 2021b, p. 1). Under the NIPP, critical infrastructures and key resource sectors include roads and bridges, chemical facilities, nuclear plants, water treatment facilities, communications, technologies, electrical power grids, and natural gas transmission lines. Under the DHS Presidential Directive 7, special consideration is given to physical security, cybersecurity, and human capital to protect the CIKR. The CIKR considerations require “effective implementation of protective programs and resiliency strategies” (Tata & DeCotis, 2019, p. 1). The NIPP requires a risk management framework that targets six areas:

1. CIKRs are required to set specific goals and objectives to manage risk.
2. CIKRs must identify assets, systems, and networks to protect.
3. CIKR must develop a risk management plan, conduct risk assessment, and assess the “consequences, vulnerabilities, and threats” (DHS, 2021b, p. 1).
4. CIKR must prioritize specific processes to protect and secure infrastructures.
5. CIKR must have formal processes to implement intervention and preventive programs.
6. CIKR preventive and security programs must be practical and measurable.

The overall process involves establishing an effective strategy for assessing risk and risk management to produce a “comprehensive, systematic, and rational assessment of national or sector risk” (Tata & DeCotis, 2019, p. 2).

Tezak (2019) noted in viewing natural gas pipelines and natural gas transmission lines issues involving these critical infrastructures are regulated by the Federal Energy Regulatory Commission (FERC; p. 209). For each pipeline construction project, operators must obtain a permit and certification. Even though the FERC is the regulating agency, additional measures are often related to land use, and particular limitations must be mitigated before construction projects can proceed. Tezak further suggested in some cases, local and state governments and non-FERC agencies may appeal decisions made under the FERC to ensure all state requirements are completed by all agencies involved in the process.

According to Bencie and Araboghli (2019), under the DHS, 16 critical infrastructure sectors have been identified as economic sectors, energy grid sectors, healthcare sectors, transportation sectors, communication networks, and natural gas transmission pipelines, and any disruption to these systems will devastate the “American way of life” (p. 40). In each sector, the DHS encourages owners and operators of CIKRs to create continuity and resiliency programs and what-if scenarios with state and federal governments' and local governments’ assistance. The process allows stakeholders to prepare for seen and unforeseen incidents and apply countermeasures to mitigate risk. Bencie & Araboghli suggested targeting domestic terrorists, violent extremists, and other threats; a target analysis and an assessment tool may be used to assess risk in qualitative and quantitative procedures. Six factors—criticality, accessibility, recoverability, vulnerability, effect, and recognizability (CARVER)—are used to assess threats:

1. Criticality: Targets “points of failure” can have the most significant liability and negative impact on operational functions.
2. Accessibility: Represents the level of ease in which an adversary will have access to the target.

3. Recoverability: Represents continuity in the ability to resume normal functions after a successful attack.
4. Vulnerability: Represents the risk factors and points of access available to the adversary to exploit facilities and information technology.
5. Effect: Represents the consequences, scope, and magnitude of disruptions and damage to facilities perpetrated by the adversary.
6. Recognizability: Represents the "degree to which an asset can be recognized as a desirable" target by an adversary for attack (Bencie & Araboghli, 2019, p. 2).

The CARVER assessment tool has been around since WWII as an offensive targeting tool to help bomber pilots target the adversary's munition sites. (Bencie & Araboghli, p. 2).

The dissertation will target how leaders in homeland security today devise processes to monitor, protect, and secure electric power grid systems, natural gas pipelines, and natural gas transmission lines identified as critical infrastructures and key resources. In addition, the dissertation will include measures to assess vulnerabilities, conduct risk assessments, and address domestic terrorism. The dissertation will be supported by the geographical information system (GIS) mapping data to highlight the importance of identifying other critical infrastructures in the local area associated with underground natural gas distribution and transmission pipelines.

As Anderson (2020) stated, in the United States, there are approximate "2.56 million miles (4.12 million km)" of natural gas pipelines, and these pipelines are responsible for carrying "natural gas to more than seventy-five million customers," including residents, businesses, and corporate organizations (p. 1873). In 2019, natural gas pipelines supported $150 billion in annual expenditures and production to support customers, utilizing gas resources for "heat, electricity, plastics, fertilizers, pharmaceuticals, fabrics, and organic chemicals" (Anderson, 2020, p. 1873).

In addition, Anderson noted that there are benefits to natural gas pipeline construction for communities.

There is risk associated with different phases of the pipeline construction and risk to communities and organizations due to leaks, threats to life, and property damage. Anderson (2020) further noted that in some communities that host natural gas pipelines, there is a reduction in property values associated with risks leak of leaks, corroded pipes, and explosions. Therefore, leaders need to understand there is an explicit and implicit cost in natural gas operations. Anderson stated expenses related to "public and private property damages and emergency response" are explicit expenses, and costs associated with personal injuries, loss of life, and deaths are implicit costs (p. 1873). Anderson further stated the PHMSA, a division of the U.S. Department of Transportation, is responsible for tracking incidents, and between 2000 to 2019, there were a total of 12,316 natural gas pipeline incidents, including "309 deaths, 1232 injuries, and $10.96 billion in property damage," reported by the PHMSA (p. 1873).

Lemos-Cano and McCalley (2019) suggest natural gas pipelines and electrical grids have future implications. The role of leaders will often require optimizing systems to meet the demands of customers and new pipeline construction. Natural gas has been an essential resource in years past, and these critical infrastructures are an integral part of the global energy landscape. Lemos-Cano and McCalley suggested preparation for future expansion; a deterministic model will require determining the type of construction, the location and capacity, and the amount of time needed in business investments, including the operational cost and security, and assessing the reliability criteria. Depending on demand and expenditures, natural gas transmission pipelines can be modeled based on the cost of improvements, "combustion turbine units, and the combined cycle plants used to generate electricity" and "representations according to the assumptions considered" (Lemos-Cano & McCalley, 2019, p. 2).

Eyberg (2019) noted that leaders and management structures associated with electric power grid systems, natural gas distribution, and oil producers are concerned about cyber-criminals because these hackers can target system networks that control production, distribution, and transmission. A report issued by the API and Oil and Natural Gas Subsector Coordinating Council indicated that securing these critical infrastructures in a "defense-in-depth" posture is a significant concern for upstream facilities, transmission, and locations that extend to wellheads, pipelines, transmission facilities, and securing construction sites (Eyberg, 2019, p. 37). To secure these operational facilities and platforms require:

1. Conducting assessments on the "less in-secure core technology" and systems(Eyberg, 2019, p. 39).
2. Upgrading "cyber-tools and techniques" (Eyberg, 2019, p. 39).
3. Creating more secure operational facilities and upgrading internet platforms and software.
4. Making natural gas pipeline investments and improvements in physical security and surveillance monitoring, biometrics, and facility security.
5. Natural gas companies invest in uni-kernels technology to create "more secure systems" (Eyberg, 2019, p. 39).
6. Uni-kernels is a software and systems upgrade that includes initiatives to assess and monitor operational and system functions.

Eyberg further suggests that securing systems and software upgrades will require expert engineers, reliable system and technology service providers, and secure internet platforms to provide real-time operational and situational analysis and include investments in uni-kernel applications.

According to Obadi and Korček (2019), the future of natural gas production and transmission will be reliant on the natural gas market, the energy environment around the world, and the strong demand for natural gas in parts of Asia. Support for energy security and demand will require investments in new natural gas pipeline infrastructures and reducing operational costs to control consumer costs. Obadi and Korček stated that U.S. natural gas production and infrastructures had met all analysts' expectations, which has led to lower natural gas prices in the past and an increase in the demand and cost in 2020 due to natural gas pipeline upgrades.

According to Kuczyński et al. (2019), in the leadership role, natural gas distribution and transmission are critical in promoting natural gas pipeline operations efficiency. Continuity is an essential factor, and some distribution points have vortex turboexpanders which depending on the transmission pipeline, can provide "high efficiency in the range of 70 to 90%" (Kuczyński et al., 2019, p. 2). Natural gas regulation stations (GRSs) can positively impact efficiency and gas facility expansion to determine selection criteria for a cost-effective application of turbo-expanders at selected GRSs (Kuczyński et al., 2019, p. 1). Improving natural gas distribution and transmission increases efficiency, and the GRSs can help determine if gas flow is too high or too low, and automatic control systems help to determine if there are problems and regulate gas flow. To improve continuity, key performance indicators (KPIs) can be incorporated into pressure reduction stations and assist in "natural gas recovery at the GRS," according to Kuczyński et al. (p. 4). Regulatory laws and statutes will require providers to ensure continuity and resiliency in natural gas transmission depending on the location of the natural gas distribution and transmission process.

According to Josephine et al. (2020), community resiliency is essential in the leadership role in electric power grid transmission and natural gas production, distribution, and transmission. Josephine et al. suggested that local, state, and federal governments must have public policies that support community plans for resiliency and continuity to protect against natural hazards and disasters. In addition, many leaders, homeland security elements, and law enforcement enhance community resilience by adopting measures, strategies, and procedures to address manufactured and natural disasters and domestic terrorist threats. Planning also includes the involvement of community residents, stakeholders, and the faith community. Planning resiliency programs have two key areas of concern:

1. Stakeholders involved in the process understand community resilience affects strengthening communities and community resources.
2. Elements of the process require mitigation, risk assessments, strategic planning, preparedness, and stakeholders' involvement is an essential part of the process.

Building community resilience is an integral part of society's protection against natural disasters and threats posed by extremist and domestic terrorists in many parts of society. It is also vital in safeguarding soft targets such as natural gas pipelines and electric power grid transmission lines and facilities from domestic terrorists and acts of terrorism. Scripture teaches, in many elements of life as seen today, "Do not be conformed to this world but be transformed by the renewal of your mind, that by testing you may discern what the will of God is, what is good, and acceptable and perfect (*King James Bible*, 1769/2021, Romans 12:2).

Cantelmi et al. (2021) explained that in management structures in homeland security, resiliency is an essential factor that recognizes the ability of critical infrastructures (CI) to recover from threats and vulnerabilities, disruptive and destructive events, as well as reduce the level of shock systems can absorb during operational functions. In homeland security, processes to ensure risk assessments and management measures are based on resiliency in the level of "robustness, redundancy, resourcefulness, and rapidity" (Cantelmi et al., 2021, p. 342). These measures are incorporated into the technical capabilities, communication and system networks, transmission, distribution, and organizational and social aspects of the organization. Cantelmi et al. suggested PRAs and risk analysis can provide data from interviews, questionaries, observations, and methods used in resilience research from detailed best practices and lessons learned from current and previous research studies. Cantelmi et al. discussed a systematic review based on preferred reporting items for systematic reviews and meta-analyses (PRISMA) in quantitative research can help to determine the principal level of dimensions relative to critical infrastructure associated with "techno-centric, organizational, community, and urban resiliency" (Cantelmi et al., 2021, p. 344).

Around the world, critical infrastructures and key resources have great significance, and infrastructures, in some cases, are identified according to public use in society (Derks et al., 2020). For instance, forest preserve areas and parks are considered infrastructures in Bonn, Germany. During the COVID-19 pandemic and the lockdown in 2020, the government "restricted citizen freedom of movement and assembly" (Derks et al., 2020, p. 102253). The COVID-19 pandemic provided forest management the opportunity to assess and engage with visitors and measure the reactions of citizens that flocked to forest recreation areas. Although, in one qualitative research study, Derks et al. noted that "the influx of visitors posed challenges for forest managers and was contrary to urban forest policy," pandemic response efforts and research findings suggest the pandemic increased visitors (p. 102253). Derks et al. indicated before the COVID-19 pandemic, there was an average of about "290 people per day" that visited forest infrastructure, and qualitative research study findings indicated, “the vast majority of visitors were over 40 years old, and 80 percent of visitors were born before 1980” (p. 102253). However, during the pandemic between March 2020 and April 2020, the number of visitors visiting forest preserve infrastructure increased to “690 visitors per day,” according to Derk et al. (p. 102253). They recommended future research studies help determine visitor preferences and why visitors are motivated to visit forest preserve infrastructure even if there is a pandemic or other emergencies.

Awuzie and Monyane (2020) explained that some delivery systems identified as critical infrastructures must have sustainability in parts of society because negative influences can significantly impact these systems. According to Awuzie and Monyane, the ability to function correctly and mitigate these concerns requires a governance framework design to help guide project managers to develop effective “sustainable project management practices” (p. 961). Today, advancements in technology require upgrading infrastructure to mitigate threats, vulnerabilities, risks, and the level of pressure placed on natural ecosystems and infrastructure upgrades in electrical grids and natural gas pipelines infrastructures must be in line with the “pace of technological transformations” in modern society (p. 961). Awuzie and Monyane further noted infrastructure client organizations (ICOs) have an essential role in devising ways to increase the amount of investment in critical infrastructures, assets, and processes that are essential in promoting “comprehensive adherence to the sustainable development goals” (SDGs; Awuzie & Monyane, 2020, p. 961). Research data are collected on quantitative data, and qualitative multicase studies conducted for qualitative content analysis (QCA) are used to evaluate data obtained from sampled and structured interviews to help determine the level of infrastructure sustainability, according to Awuzie and Monyane (p. 961).

According to Kruglanski et al. (2020), during the COVID-19 pandemic in 2020, no indicators suggest the pandemic impacted terrorist activities. There was no decline around the world in international and domestic terrorism. Even though the COVID-19 pandemic impacted many people and societies, institutions were still being exploited by jihadists, left-wing extremists, and far right-wing extremists who spread propaganda and conspiracy theories. In viewing aspects of extremism, domestic terrorism, and international actors in America during the COVID-19 pandemic, there were the following incidents:

1. Domestic terrorist-related incidents involving "fifty vehicles ramming attacks since late May that targeted protesters" (Kruglanski et al. (2020, p. 121).
2. Domestic terrorist groups such as the Boogaloo Boys far-right extremist group intensified domestic terrorist attacks, instigated propaganda attacks against the pandemic lockdown, and promoted anti-lock-down and police brutality protests and demonstrations in many U.S. cities.
3. Anti-Asian hate crimes increased early in the pandemic.
4. Far-right extremist groups and organizations such as Qanon, Oath Keepers, Proud Boys, Boogaloo Boys, and others were "responsible for 90% of domestic terrorist attacks in the U.S., in 2020, compared to 66% in 2019' (Kruglanski et al., 2020, p. 121).
5. Far-left extremist groups such as Antifa were responsible for violent and destructive demonstrations supporting some liberal viewpoints and protested during BLM rallies and police brutality demonstrations.

Kruglanski et al. also noted that there were anti-lock-down protests and increased cyber-attacks designed to target hospitals and medical facilities in other countries, such as Germany.

Moreover, in many parts of society, international and domestic terrorists sought to use the pandemic to grow stronger and exploit gaps in security and as a means to “forward their ideologies as a substitute for fear, frustration, and panic,” according to the authors (Kruglanski et al., 2020, p. 122). For some domestic terrorist groups and organizations during the COVID-19 pandemic, it has been opportune to bolster messaging and spread propaganda to support extremist political viewpoints, recruit new members, incite violent extremist acts, and further the agenda of the organization.

Theoretical and Conceptual Framework

According to Maertens et al. (2022), the Bayes theorem was first introduced in probability theory and statistics by mathematician Thomas Bayes around the 17th century. This theoretical perspective explains aspects of probability and how it relates to an event or phenomenon based on calculating the frequency of an event and the available knowledge of conditions before the event occurs. Bayes developed a mathematical process for inductively assessing probability and established probability interference to calculate probability and validity. Maertens et al. explained that in safety sciences, examining probabilities allows researchers to explore uncertainties, risk assessment factors, and worst-case scenarios and develop better ways to conduct risk assessments. Maertens et al. suggested that the Bayesian approach and PRA methods help leaders improve on making decisions in risk management processes and transition from traditional processes to new methods based on evidence-based processes and integrating data in engineering exercises. From the theoretical perspective, randomness plays a significant role in computing predictions based on data and prior knowledge of an event or phenomenon. Maertens et al. discussed the term “probability” represents the ability to rely on partial knowledge, and uncertainties in risk analysis can provide:

1. Scenario uncertainties are directed toward omissions that can be incorrect or incomplete specifications of the risk scenario.
2. Model uncertainties represent expressing limitations in the mathematical models or calculating techniques.
3. Input or parameter uncertainties are representations of uncertainties related to measurement errors that must be taken into consideration systematically based on bias in data and randomness.

Determining probability in risk assessments is also reliant on the methodology used to measure outcomes and potential consequences associated with an event, phenomenon, behavioral characteristics, and certain factors related to critical infrastructures in homeland security.

Jiang and Liao (2021) suggested variables related to probabilities that require addressing the research gap. To bridge the research gaps, "linguistic variables and multi-granularity linguistic term set," researchers must use a "double-quantified linguistic variable to qualify two forms of language representations" (Jiang & Liao, 2021, p. 207). The first involves linguistic variables must consist of probability information, and the multi-granularity linguistic term set must have correct probable information to identify the differences in shortages in a "multi-granularity linguistic term set" (Jiang & Liao, 2021, p. 207). An example is that a natural language can be ill-defined as expressing probabilities in a humanistic system and serving as a means of communication for people. However, too few probability mechanisms, such as computers, can directly handle human language because computers are "governed by the laws of mechanics, physics, chemistry, and electromagnetism" (Jiang & Liao, 2021, p. 207). Therefore, there must be a representation of variables to consider linguistic variables. The values must involve words, phrases, and sentences in artificial and natural language form or consist of numbers in a specific range. When there are linguistic representations and variables, probability can be used to make various comparisons associated with an evaluation, event, or phenomenon based on certain known factors.

In the field of homeland security, according to Nagin (2013), the deterrence effect is a factor that can potentially help prevent recidivism in the criminal justice system. The probability of apprehension is a factor related to domestic terrorists, violent extremists, and cyber-criminals when there is a certainty of apprehension and a lengthy prison sentence. Probability has a role in homeland security and the criminal justice system when it can contribute to the deterrent effect. In viewing probability and deterrence, four research gaps should be taken into consideration:

1. The first is related to the mechanisms available to law enforcement to change the perception of the probability of apprehension.
2. The second involves the link between the deterrence effect and the threat of severe punishment and the "criminogenic effect of the experience of punishment" (Nagin, 2013, p. 199).
3. The third is the probability of the concept of a sanction regime, and legal authority is measured to contribute to the deterrent effect.
4. How does sanction risk relate to probabilities in the criminal justice system?

Nagin suggests based on the probability of apprehension, if the four research gaps are not addressed and if a link is not established between risk perceptions and imperative sanctions, there is no way to adjust perceptions if the punishment is not severe, however, cruel, and if "changes are not made in punishment and sanctions the deterrent effect will not be achieved" (Nagin, 2013, p. 199). Nagin further suggested in a framework in the criminal justice system and homeland security, if probability measures are correct, the consequences will provide certainty of apprehension when there are more legal consequences, lengthy sentences, and severe punishment, and the deterrent effect can be achieved.

Summary

The conceptual and theoretical framework in the dissertation will be structured around PRA in management structures in homeland security and protecting critical infrastructures. According to Ekström et al. (2021), a conceptual framework or concept involving a PRA should include a method for risk analysis in a scenario or simulation design to provide building blocks to optimize the design criteria. The risk analysis and criteria will allow decision-makers and stakeholders to make informed decisions based on evidence-based data and provide a comparative analysis and optional models in building specific designs and patterns that highlight values and a consequence model to help avoid consequences associated with not complying with energy requirements. A conceptual framework or concept can include two design models directed toward the "probability of failure and the probability of different design options" and should reference cost-effectiveness and is financially viable (Ekström et al., 2021, p. 111434). Probabilistic risk analysis should consist of an iterative process that involves steps to be performed, an analysis, and data input. Each facet of the iteration process should contribute to more complexity, add to the building blocks, and provide substantive data to help inform decision-makers, according to Ekström et al. In homeland security elements and critical infrastructure, a conceptual framework can include six steps that suggest the following:

1. Design plans should first define and identify stakeholders (government entities, contractors, developers, agencies, and community stakeholders) in building a critical infrastructure framework for new developments, technology, and upgrades.

2. The second step can include factors identification which references identifying influences, identifying uncertainties, and identifying factors that impact, quantify and evaluate design patterns.
3. The third involves the framework that can identify uncertainties and what qualifies as uncertainty and provide a probability distribution that references uncertain perimeters based on data.
4. In the building design input data, sampling and random sampling should be part of the process.
5. There should be simulations that highlight "multiple simulations and calculations, depending on the chosen models, there can be two datasets per design option, and highlights stochastic parameters" (Ekström et al., 2021, p. 111434).
6. The sixth step involves a framework for critical infrastructures that should provide energy performance (EP) data to help determine EP feasibility, uncertainty, and EP variations, according to Ekström et al.

Ekström et al. explained that the conceptual model should allow stakeholders and decision-makers to evaluate and validate the PRA and examine all probabilities. For example, a case study can be used to validate probabilities, phenomena, values, or factors related to construction or distribution, building processes, energy performance, or how a specific infrastructure functions in real time.

According to Jaimes et al. (2020), a PRA framework can be used to compare and evaluate the economic outcome of "wind turbine towers subjected to cyclone-induced wind loads" is applied (p. 528). The conceptual framework should consider all probabilities, uncertainties, and the consequences of cyclone-force winds and specific hazards. Significant factors in the assessment include identifying wind speed, wind direction, risk perimeters, vulnerabilities, and the economic cost to the organization and consumers. Another key indicator is the geographic locations in which wind turbine towers are located are in making comparisons between electric power grid systems and power distributed from nuclear power plants. One of the goals of the PRA is to assess the "probability of negative consequences" (Jaimes et al., 2020, p. 529).

Saada (2021) noted a probability theory could be used in conjunction with the Bayes theorem, a statistical process that examines the probability of a different set of causes and help to project the outcome when data is computed to measure the consequences and outcomes. The probabilistic graphical model (PGMs) is a process that seeks to "provide complex multivariate systems as joint probability distributions" because it is used to make comparisons between "multidimensional space based on natural and intuitive variables" (Saada, 2021, p. ii). On the other hand, dynamic Bayesian networks and Bayesian inference techniques are processes used to compare reasoning over certainty in probabilities when projecting "domains of human activity recognition and detection," which can potentially be essential in counterterrorism in tracking patterns in human activity and behavior and computer interactions and activity on video surveillance systems (Saada, 2021, p. ii). According to Montag et al. (2021), the dynamic Bayesian network theory was created in the 1990s by Dr. Paul Dagum at Stanford University, and today the theory is applied in research to study "digital biomarkers of brain function" in mental health to identify continuous markers (p. 897).

Christian Perspective and Homeland Security

According to Xiong et al. (2020), a Christian perspective on homeland security can provide leaders with spiritual guidance for addressing challenges and problems associated with the COVID-19 pandemic and domestic terrorism from a practical and spiritual perspective. Xiong et al. explained that spiritual practitioners consider the COVID-19 pandemic from a theological lens and rely on faith and spiritual resources to overcome these challenges. In addition, people of faith and spiritual care providers practice self-care to help overcome challenges until they can receive COVID-19 vaccinations. Today, while the challenges and problems related to the COVID-19 pandemic have been overwhelming, vaccinations are now available, and people are encouraged to get vaccinated.

Xiong et al. (2020) further noted many people feel the "pandemic and emergency preparation capacity, and rapid response" is essential and a priority (p. 16). For many people, spiritual light has shone through the darkness brought on by the pandemic, and there will be lessons learned "not only as nations to nations but also as humans to all sentient beings and the living conditions surrounding us" (Xiong et al., 2020, p. 18). In many ways, the COVID-19 pandemic has changed the way people live. In years to come, in research to address gaps related to the COVID-19 pandemic, lessons will be learned from the tragedy and lessons shared by many nations. In society today, many "Christians are feeling the heaviness of the pain and suffering being experienced by humanity" (Xiong et al., 2020, p. 23). Many people are discovering the "body of Christ" and questioning how they can remain a community of faith if people are forced to stay in isolation (Xiong et al., 2020, p. 26). Future research will show how Jesus Christ died for the sins of many, and "today we know that Jesus too has been there, alone in the tomb; his family and friends separated from him as well" (Xiong et al., 2020, p. 27). Scripture teaches, "For by one Spirit are we all baptized into one body, whether we be Jews or Gentiles, whether we be bond or free; and have been all made to drink into one Spirit" (*King James Bible*, 1769/2021, 1 Corinthians 12:13).

Kessler (2020) noted that effective leadership transforms the world, and servant leaders serve others. Therefore, Christian leaders should fight against ugliness in the world and strive to "make the world more beautiful" (Kessler, 2020, p. 1). Kessler noted the link between "aesthetics and transformation of the world" in Christianity (p. 1) and recognizing God as the head of the church. Transformational-servant leadership recognizes:

1. In representing the Body of Christ, leaders must go beyond the church.
2. Leaders must strive "for truth and the goodness" in representing Christ Jesus (p. 1)
3. Leaders must understand that "the spirit is the real leader of the church" (p. 1).
4. In the workplace and community, servant and spiritual leaders "partake in the work of the Spirit" (p. 1).
5. Spiritual transformation is caring for others and "beautifying the church and beyond" (p. 1).

Kessler further noted that in the church, transformative leaders are the link between leadership and beauty in rediscovering the "beauty in the church leadership office" (p. 1). Christian spirituality is about leading the church and church organizations to serve the community and help others. Transformation takes place when people find their way to God through beauty and Spirit. Because what gives people the most "pure authentic feeling" is transforming and witnessing God's presence (Kessler, 2020, p. 2). The Bible teaches, "All Scripture is breathed out by God and profitable for teaching, for reproof, for correction, and training in righteousness, that the man of God may be competent, equipped for every good work" (*King James Bible,* 1769/2021, 2 Timothy 3:16-17).

CHAPTER THREE: METHODOLOGY

Overview

Chapter Three includes a presentation of the research methodology, consisting of data collection methods, instruments, case studies, scenarios, and research participants. In addition, the chapter outlines the research questions and hypotheses of various outcomes and scenarios relevant to probabilistic risk assessments (PRA) related to homeland security and critical infrastructures involving electric power grids and natural gas pipelines and mitigating external and internal elements of domestic terrorism in America. The PRA process involves examining conditional probabilities related to the outcome of an incident or stated cause.

Design

According to Hayes (2022), in the case of "independent probabilities of A and B, an equation will be equal to P(A) and P(B)" (p. 1). The overall purpose of the Bayes theorem and rule is to provide a mathematical computation to assess conditional probability when it involves the probability of an event (A) occurring versus an event (B) that already has occurred based on predetermined conditions. This process can also include variables and observations associated with an event or occurrence.

The research design will consist of several theoretical perspectives related to PRA and Bayes's theory, developed by and named after Thomas Bayes (c. 1701–1761). The theorem was developed to understand probabilities related to an event and based on prior knowledge of the conditions of the event. In some instances, the theory is applied to statistical inferences in data and statistical analysis and probability interpretations to measure an event or occurrence and how an incident may occur. In homeland security (HLS), critical infrastructure and key resources are essential to basic human needs, economic sectors, technology, operational functions, and system networks. The design is essential because critical infrastructures (CIs) must receive adequate protections to protect against natural and man-made disasters, cyber-threats, external and internal domestic terrorism in America.

According to Suo et al. (2021), because CIs provide equally significant social public services, ignoring probabilities, risks, and vulnerabilities can lead to extensive damage and a loss of essential resources and services. CIs also provide resources such as natural gas, electricity, and water and support communication and transportation systems needed to support the quality of life in many communities. In infrastructures, the quantitative PRA model provides measurements of risk occurrence and can be instrumental in assessing other risks, providing a risk profile, and assessing and identifying weaknesses in CIs. The CI framework can include three factors related to risk factor multiplicity, CI interdependency, and dynamic stochasticity and characteristic that renders "CIs' risk more susceptible to variability and uncertainty," and risk conditions qualified by probability and loss (Suo et al., 2021, p. 1.). In addition, quantitative measurement requires determining the level of risk-alert periods and determining if the risk is high frequency. Suo et al. (2021) noted that in creating a PRA scenario for CIs, a multidimensional analysis includes the scenario elements, evolution, and effect. A scenario-driven dynamic stochastic model (SDDSM) comprises a 3-step solution and provides a rating of the risk based on the dynamic stochastic probability of the risk and independent CIs and the classification of risk identified in the scenario. The design features of the model and the multidimensional PRA analysis should include three elements:

1. Elements of the scenario can include multiple risk factors and multiple interdependent CIs and include variables, components, and classifications, and qualifying factors associated with risk can include the following:

a. Hydrometeorological hazards and terrorist-related incidents,

b. Pipeline failures and power outages, and

c. It includes classifying sources of risk factors such as natural and man-made disasters and internal risk factors.

2. The scenario evolutions represent the mechanisms in the dynamic stochastic model and are related to the following:

   a. How risk factors change “dynamically and appear or disappear stochastically” (Suo et al., 2021, p. 2),

   b. Whether or not risk factors worsen or the type of targeted measures are used to reduce the effect or control the situation and the frequency of the occurrence.

   c. The evolution of mechanisms is reliant on the status of multiple conditions related to operations and system functions, “normal operations, disruptions with or without restoration, failures, recoveries, and the establishment of a new normal” (Suo et al., 2021, p. 2), and the level of resiliency and redundancy

3. The scenario effect in the PRA scenario process represents summing up risk and showing how there are interactions between individual and single risk. The scenario effect processes include the following:

   a. The CI aggregation risk factors must demonstrate multiplicity and interdependency, and

   b. The CI aggregation should demonstrate how risk is classified, representing two types of risk series and parallel.

According to Suo et al., a research design that highlights aggregated CI risk factors that are often referenced in other existing research studies related to CI probability risk factors should include the following:

- Natural risks: Risk factors related to “earthquakes, hydrometeorological hazards, hurricanes, flood plain areas, and climate change” (p. 2).
- Man-made risks: Risk factors associated with “construction damage, acts of terrorism, intentional malevolent acts, cyberattack, external disruptions, human error, and data breaches (p. 3); and
- Internal factors: Risk factors due to flaws considered as defects in the design, pipeline valve failures, system blockage failures, aging infrastructure, and failures in the electrical power grid systems.

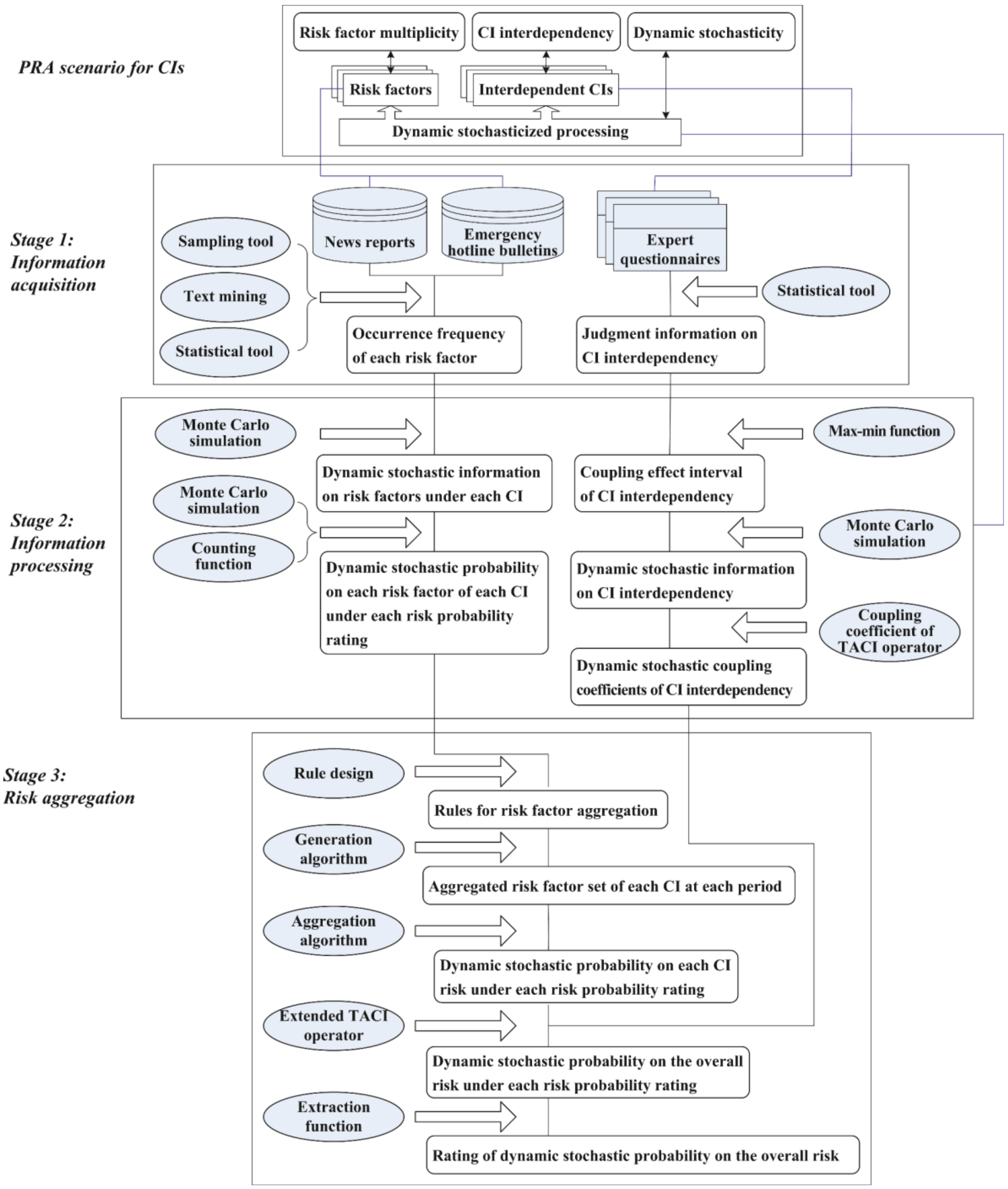
CI Interdependency Classifications

- Geographical problems, physical security, cyber security, and “logical interdependencies,
- Input, mutual, shared, exclusive, or collocated interdependencies, and spatial and functional interdependencies,
- Budgetary and market interdependencies, and stochastic interdependencies” (Suo et al., 2021, p. 2).

CIs have become more prevalent in many parts of society and require quantitative measurements of specific risk and risk occurrence probability, identifying vulnerabilities and weaknesses, supporting the risk profile, and planning preventive strategies to mitigate probabilities and risk. In Figure 1, the framework illustrates a PRA scenario for CIs based on a 3-stage resolution (Suo et al., 2021, p. 5).

Figure 2

PRA Scenario for CIs


PRA scenario for CIs
Risk factor multiplicity
CI interdependency
Dynamic stochasticity
Risk factors
Interdependent CIs
Dynamic stochasticized processing
Stage 1: Information acquisition
Sampling tool
Text mining
Statistical tool
News reports
Emergency hotline bulletins
Expert questionnaires
Statistical tool
Occurrence frequency of each risk factor
Judgment information on CI interdependency
Stage 2: Information processing
Monte Carlo simulation
Max-min function
Dynamic stochastic information on risk factors under each CI
Coupling effect interval of CI interdependency
Monte Carlo simulation
Counting function
Monte Carlo simulation
Dynamic stochastic probability on each risk factor of each CI under each risk probability rating
Dynamic stochastic information on CI interdependency
Coupling coefficient of TACI operator
Dynamic stochastic coupling coefficients of CI interdependency
Stage 3: Risk aggregation
Rule design
Rules for risk factor aggregation
Generation algorithm
Aggregated risk factor set of each CI at each period
Aggregation algorithm
Dynamic stochastic probability on each CI risk under each risk probability rating
Extended TACI operator
Dynamic stochastic probability on the overall risk under each risk probability rating
Extraction function
Rating of dynamic stochastic probability on the overall risk

Suo et al. (2021) further noted that some CIs classifications are based on risk factor multiplicity and may include hybrid models designed to function as the PRA model representing electrical power grid systems. The cumulative effect and creating risk curves are based on probabilities representing system failures, and quantitative measures justify probability and loss. The illustration in figure 1 highlights procedures for framework and procedures on quantitative measurements. The PRA framework for three-stage CI scenarios is represented by:

1. The first stage is information acquisition, in which information and data are gathered from "objective factual CI interdependency information and records based on the subjective expert judgment" (Suo et al., 2021, p. 4).
2. The second stage involves assessing and processing the frequency of information provided on risk, and "CI interdependency information is processed dynamically and stochastically, corresponding to dynamic stochasticity" (Suo et al., 2021, p. 4).
3. The third stage is risk aggregation, considered a "hierarchical risk aggregation" process designed to identify risk factors and CI risk aggregations (Suo et al., 2021, p. 4).

A dynamic stochastic model is used as a scenario to support a PRA for interdependent critical infrastructures and provide a basis for disseminating critical information.

According to Chalgham (2020), in creating a PRA design and model for addressing pipeline failures, a system-level prognosis, and health monitoring (PHM) methodology to mitigate pipeline health and failures. Furthermore, providing a comprehensive approach to natural gas pipelines require strategies designed to provide measures in pipeline maintenance of various components and systems and provide strategies to address pipeline degradation and mitigate the cost of maintenance programs and operational and economic cost factors. Additional

PSA measures can include optimizing safety protocols and environmental factors and upgrading sensors in locations in the pipeline to maximize protection. The PHM is a methodological design that can effectively optimize operational performance and provide practical strategies for mitigations. Chalgham explained that enhancements and mitigations in a PHM model help protect the integrity of pipeline systems and reduce pipeline degradation and failures related to interdependencies and system components. The PHM is designed to

- Optimize system health and "reliability in real-time and over-time" (Chalgham, (2020, p. 14).
- Optimize how system components function, perform and manage structures, and schedule pipeline maintenance.
- The PHM process will help optimize the placement of health sensors through the pipeline for preventive detection measures, perform diagnosis on valves, and provide predictive measures to assess failure causes of gas pipelines.

Chalgham further noted that the PHM design and methodological approach is essential for management structures to support the integrity of the pipeline system and is a proactive approach to mitigate challenges and problems and avoid system-level failures through mitigations. Therefore, in a PHM framework and model, system-level performance is essential and represented by three functions:

- Provide mitigations for pipeline corrosion,
- Provide a model and methodological approach to pipeline degradation, and
- Provide a process model that mitigates challenges and problems associated with compressors and valves.

In addition, to address degradation in natural gas pipelines, a system-level functional model may include the “Fault tree or a Bayesian network” (Chalgham, 2020, p. 20) that assesses the functional degradation and add to reductions in the performance of compressors.

Research Questions

Research Question 1: Analysis

RQ1: What is a theoretical approach to a probabilistic risk assessment (PRA) in homeland security?

According to Chatterjee et al. (2021), in viewing PRAs from a theoretical perspective, PRA is commonly used in the HLS field to assess and evaluate failures in systems and networks. In homeland security, PRA is a process that can be integrated into risk management and concepts of resilience when there are incidents and occurrences involving uncertainty and risk. Chatterjee et al. noted that from a theoretical perspective, PRAs provide a “direct way of modeling stochastic resilience measures” (p. 369) and include different variables or resilience metrics to apply the Bayesian statistical process to assess uncertainty, level of threat, and vulnerability. In HLS, scenarios are created to assess and model risk, vulnerabilities, and uncertainty; and use simulation tools to help model specific conditions and occurrences and assess the impact of the event type and the severity associated with a system and operational failure and outcome. In addition, PRA theoretical perspectives provide an approach to risk analysis on resiliency and methods that can “integrate vulnerability and resilience dimensions into the risk assessment processes” (Chatterjee et al., 2021, p. 369). According to Chatterjee et al., in PRAs, a scenario and simulation-based approach to risk assessments can quantify data and integrate uncertainties in Bayesian networks and Monte Carlo simulations in processes designed to produce resilience metrics and probability distributions.

Research Question 2: Analysis

RQ2: How are probabilistic risk assessments (PRA) applied in risk management?

According to Thöns and Stewart (2020), PRAs can be a significant part of risk reduction strategies in homeland security to help prevent terrorist attacks and acts of terrorism by modeling activities related to improvised explosive devices involving “large governmental building structures” (p. 1). To help determine cost-efficiency, assess the significance of an event or occurrence, and take measures toward safety and protecting life. In addition, the “Bayesian pre-posterior decision analysis” informs decision-makers on prior information (Thöns & Stewart, 2020, p. 1) and new knowledge to make more informed decisions in risk management.

Research Question 3: Analysis

RQ3: How are probabilistic risk assessments (PRA) used to compare risk in critical infrastructures?

According to Nouri Qarahasanlou et al. (2021), a comparison of PRAs is reliant on the number of risk factors and the level of “CI reliability (uptime) and recoverability (downtime) performance” (p. 2). The processes require using “probabilistic performance measurement tools” (p. 2). In comparing CIs, recoverability, is a term representing a system’s ability to perform under various conditions and based on time intervals, disruptive events, and external resources. Furthermore, in comparing CIs, the restoration process is viewed as a joint probability when factors are based on the “event, correct prognosis, diagnosis, and mitigation and recovery” as follows: “Re = R + (1 - R) P-diagnosis / P-prognosis and P-Recovery” (Nouri Qarahasanlou et al. (2021, p. 4).

Nouri Qarahasanlou et al. (2021) further noted that comparisons are determined based on performance metrics and the following equation: “p-diagnosis represents the probability of correctness, p-prognosis probability is the measure of correct prognosis, and the probability of correct recovery is represented by p-recovery" (p. 4).

According to Nouri Qarahasanlou et al. (2021), a comparison can be made in CIs if the framework and methodological approach is designed to provide a risk factor-based reliability importance measure (RF-RIM). A process that evaluates probabilities and risk to measure the level of resilience and "sum of reliability and recoverability" (Nouri Qarahasanlou et al., 2021, p. 1). In some instances, the Akaike information criterion (AIC) and the Bayesian information criterion (BIC) may be selected to determine the best fit by comparing values based on "comparing the maximum likelihood value to select the appropriate model" (Nouri Qarahasanlou et al., 2021, p. 9).

Hypotheses

The null hypotheses for this study are relevant to the research questions listed below:

RQ1: What is a theoretical approach to a probabilistic risk assessment (PRA) in homeland security?

$H_0$1: Bayesian standards are applicable to PRAs, corroborating data, and a 2-step approach to testing probabilities.

According to Bowater and Guzmán-Pantoja (2019), to test a null hypothesis in an imaginary scenario in HLS, an event is represented by the extra-sensory perception in predicting an outcome or occurrence that involves "20 independent Bernoulli trials in succession" (p. 1422), A process directed toward outcomes associated with failure or success in CI elements. Each trial represents a "probability of 0.5 and y is greater than 10" (Bowater & Guzmán-Pantoja, 2019, p. 1422). To test this null hypothesis, if the "probability of a correct prediction p is equal to 0.5," chances are an individual does not have an extra-sensory perception to predict an outcome

(Bowater & Guzmán-Pantoja, 2019, p. 1422). On the other hand, in viewing an alternative hypothesis, if the probability p is more significant than 0.5, an individual may have an extra-sensory perception to support a prediction in the right direction unless the individual was disingenuous or making a false prediction. It is also assumed that the "tested statistic is $\hat{p} = y/20$ is the maximum likelihood estimator of p, the p value for this problem," it is the assumption p value is one-sided (Bowater & Guzmán-Pantoja, 2019, p. 1422). Represented by this equation. In using a 2-step Bayesian approach to measure probabilities, observation of the data can impact the level of belief when parameter θ lies in the interval $[\theta 0 - \varepsilon, \theta 0 + \varepsilon]$ but does not represent "the one-sided P-value method," as well as to the Q-value. According to Bowater and Guzmán-Pantoja, in applying the Bayesian 2-step approach, data can be corroborated with the hypothesis if "θ lies in the interval $[\theta 0 - \varepsilon, \theta 0 + \varepsilon]$" (Bowater & Guzmán-Pantoja, 2019, p. 1435). The Bayesian standards of probabilities is a "logical way to incorporate the presence of nuisance parameters" or events into two steps based on the conditions of perimeters and based on "calculations of posterior probabilities and densities in the first and second steps" (Bowater & Guzmán-Pantoja, 2019, p. 1435). Posterior probabilities represent statistical probabilities when true calculations represent a hypothesis based on relevant observations.

RQ2: How are probabilistic risk assessments (PRA) applied in risk management?

$H_0$2: The Bayesian decision theory in PRAs provides a methodology for assessing risk and making critical decisions.

According to Oates and Sullivan (2019), a PRA can be applied in risk management from a deterministic perspective. The standard methodology concerns a decision rule and probability measure based on average-case analysis (ACA; Oates & Sullivan, 2019, p.1339). Based on the Bayesian decision theoretical perspective, an average error is determined in decision-making as expected to represent loss or risk. The ACA represents mathematical computations equivalent to Bayesian decision theory and is “limited to experiments that produce a deterministic dataset” (p. 1339). In viewing a null hypothesis using the Bayesian rule in PRA, the theoretical perspective offers a methodology for statistical testing and uncertainty quantification to finding answers to complex problems and systems “at the point of applied mathematics, statistics, computational science, and application domains” relevant to risk management and other factors such as groups, methods, and task (Oates & Sullivan, 2019, p. 1340).

RQ3: How are probabilistic risk assessments (PRA) used to compare risk in critical infrastructures?

$H_0$3: The Bayesian testing (NHBT) framework is essential in comparing risk and identifying specific perimeters in the null hypothesis.

According to Tendeiro and Kiers (2019), PRA is applicable in comparing perimeters associated with two or more populations or groups. The goal is to draw data from related populations to answer questions concerning how to determine how one can believe that M0 or M1 holds” more population perimeters. To examine probabilities, consideration given to customary ratios of probabilities and the odds ratios has been exhaustive. Tendeiro and Kiers noted that to quantify “prior odds ratio to the posterior odds ratios,” the data and statistic illustrated. The posterior probability of a model will express the prior probability to produce “the likelihood of data under the new model” (p. 774). The null hypothesis testing, or null hypothesis Bayesian testing (NHBT) framework, uses “Bayes factors to compare a point null model” by identifying a perimeter of interest with neutral value and probability density functions (Tendeiro and Kiers, 2019, p. 775). The process can be used to compare and observe data from two competing models, and the newly observed data and statistics are updated in the NHBT framework.

Case Study: PRA Bayesian Networks and Dynamic Stochasticity Models

In one case study concerning the dynamic stochastic model in measuring and assessing the risk associated with the PRA, Suo et al. (2021) used the dynamic stochastic probability to assess risk factors during a specific period. In this approach, a test determines how the model effectively identifies and tracks risk-alert periods and risk factors related to CIs and determines the model's impact on preventive measures. Other significant factors related to CI safety are determining the risk periods associated with classifying risk and providing recommendations for future support for CI plans and risk preventive measures. According to Suo et al., the information further suggests this model is most appropriate and instrumental in providing a "scenario-driven dynamic stochastic model" (p. 12). Therefore, it is suitable for decision-makers to use a PRA model to assess CI risk and determine the preventive measures needed to protect against CI risk and mitigate any concerns. Furthermore, research should examine the future implications of this model by introducing "mature theoretical tools and integration of intelligent technologies" to assess future PRA models for critical infrastructure (Suo et al., 2021, p. 12).

According to Kammouh et al. (2020), in applying the PRA probabilistic framework and design to Bayesian and dynamic Bayesian networks (BNs) and scenario-driven dynamic stochastic models, these processes can help evaluate resilience indicators and assess the resilience in engineering systems (p. 1). The BN can help determine the relationship between CIs and the indicators and handle various terms related to dependencies and variables associated with CIs in probabilistic risk factors in PRA terms. In the dynamic BN network, this model is designed to provide a more accurate picture by recording time and variables to establish the current level of resiliency in dynamic engineering systems (DES). To measure the level of resilience in these systems, a mathematical process is applied based on certain factors to determine the level of resiliency and establish the evolutions in system processes and performance. According to Kammouh et al., probabilistic methods are more appropriate in modeling engineering systems, especially in the instance when data are not available, and measurements will require the “use of a fuzzy analysis and Bayesian Networks (BNs)” (p. 2). Fuzzy theories consist of methods used when uncertainty and vagueness are uncertain, and specific factors are unclear.

Furthermore, this theory is heavily reliant on subjectivity when data are limited, or there is a lack of data, and preference is given to opinions somewhat instead of data. Nevertheless, this approach can calculate BN resilience between CIs interdependencies and require a probabilistic methodology that calculates resilience metrics and value. In addition, it can require developing a “universal resilience metric for infrastructure systems” (Kammouth et al., 2020, p. 2). A goal of the scenario-driven dynamic stochastic model is to determine factors related to the risk-alert period and high-frequency and high-risk CIs, according to Kammouh et al. (2020).

According to Kong and Simonovic (2019), there can be temporal and spatial relationships in infrastructure systems. Analyzing hazards requires assessing multiple hazards that impact CIs and the probability of damage and destruction. In cases where interdependencies represent multiple CIs, the hazard period and time variance are significant factors requiring examining occurrence probabilities. The two main types of temporal relationships are associated with how multiple hazards coincide with more than one hazard and require understanding the sequence of multiple hazards and triggers. Spatial relationships are related to the impact of multiple hazards on CIs when geographic interactions evolve. Kong and Simonovic noted that spatial relationships have recently become the focus of research studies. However, this approach relies on CI exposure to multiple hazards in limited areas of concern. In spatial relationships, factors related to the following:

- The impact of multiple hazards,
- The possibility of multiple hazards in a geographical area, and
- The susceptibility of CIs to joint impacts and secondary hazards.

In temporal and spatial relationships in CIs, there may be a "combination of conditional and joint damage probabilities caused by individual hazards," and probability damage to CIs may exceed a specific threshold (Kong & Simonovic, 2019, p. 1855).

According to Kumar et al. (2020), electric power systems (EPS) are an essential part of generation transmission distribution (GTD) networks. Therefore, they must undergo a reliability evaluation in planning and operations to help determine the level of reliability, especially in cases where there are interdependencies in power systems that support other networks. When there is uncertainty and power systems are unreliable, decision-makers encounter fuzzy figures. Uncertainties can be modeled using probability density functions (PDFs) and analyzed using the Monte-Carlo simulation (MCS) method to evaluate the reliability indicators and include point estimate methods. At least 14 work considerations apply to creating a CI training scenario to assess reliability in electrical power systems and reliability evaluations.

According to Kubo et al. (2022), in conducting a deterministic risk assessment for CI such as nuclear power plants, a PRA is used to assess and evaluate safety conditions and conduct a regulatory inspection. However, Kubo et al. noted a difficulty involved in the method related to how temporal information is handled to evaluate and monitor conditions and is "essential for modeling operators' recovery actions and level 2/3 PRA inputs" (p. 357). For example, when this process is involved in some nuclear facilities, “temporal information incorporated to provide time-dependent epistemic and aleatory uncertainties into a thermal-hydraulic (T-H) analysis” (Kubo et al., 2022, p. 357). In addition, in some institutions, a dynamic PRA can involve a “RAVEN code which is an acronym for “reactor analysis and virtual control environment” assessment (Kubo et al., 2022, p. 357), and can involve Latin hypercube sampling methods (LHS) and adaptive methods for sampling conditions.

In further viewing the role of probabilistic safety assessments (PSA), it is a systematic methodology applied in the nuclear industry to evaluate risk and provide insights into safety designs and operational functions in the nuclear power plant (NPP) industry (Zhou et al., 2021, p. 2). In measuring risk numerically, scenarios can be assessed according to consequences and frequencies on three levels. The three PSA levels that represent the following:

1. Risk and incidents associated with the nuclear reactor core,
2. Accidents or incidents related to the release of radioactivity within a facility can impact the environment and humans, and
3. The release of radioactivity or radioactive waste can result in “harm to human health and environmental damages, respectively” (Zhou et al., 2021, p. 1).

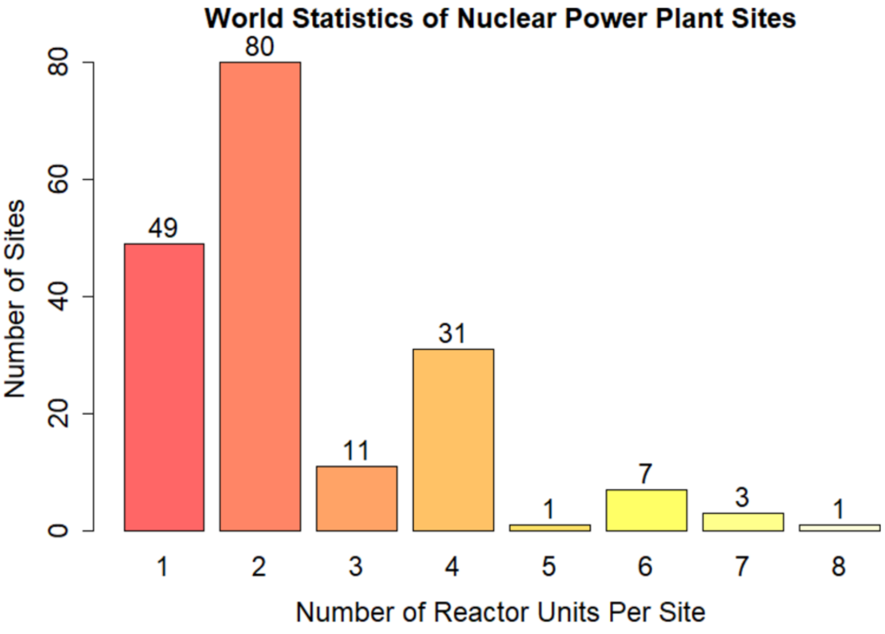
Zhou et al. noted that some conventional PSA studies generally involve single-unit PRAs (SUPRAs; p. 1), meaning studies involving scenarios on a single reactor unit as long as other units are not in a critical state and are not dependent on other reactor units. However, since the Fukushima Daiichi accident in March 2011, in conducting scenarios in nuclear facilities involving interunit dependencies, there has to be a proper characterization of risk and site-level dependencies to provide an accurate picture of the risk profile (Zhou et al., 2021, p. 1). In conducting a PSA data analysis, according to a statement by the Power Reactor Information

System (PRIS) of the International Atomic Energy Agency (IAEA) in 2020 (Zhou et al., 2021, p. 2). Figure 2 represents a statistical illustration and characterization of NPPs worldwide that highlights 442 nuclear reactors in current operation (Zhou et al., 2021, p. 2):

- Worldwide, “73.2% of these nuclear power plant sites have two or more nuclear reactor units” (Zhou et al., 2021, p. 2).
- Multiunit sites are responsible for “88.9% of the operating reactors” (Zhou et al., 2021, p. 2).
- Worldwide, 23.0% to 43.7% of sites account for two-unit sites and have two to four reactor units.

Figure 3

World Statistics of Nuclear Power Plant Sites as of April 2020



Note. From “Multi-Unit Nuclear Power Plant Probabilistic Risk Assessment: A Comprehensive Survey, by T. Zhou, M. Modarres, and E. L. Droguett, 2021, *Reliability Engineering & System Safety*, *213*, Art. 107782, p. 10 (https://doi.org/10.1016/j.ress.2021.107782).

In conducting a PRA risk assessment, there are differential factors related to a "multiunit PRA (MUPRA) and single-unit PRAs (SUPRAs)" in nuclear power facility environments (Zhou et al., 2021, p. 10).

- Multiunit PRAs are factors related to reactor dependencies at the exact location.
- Site-level PRAs these factors include all radiological dependencies at the same site and include "reactor units, spent fuel pools, and other radioactive waste storage facilities" (Zhou et al., 2021, p. 3).
- Regional-level PRAs involve radiological sources located across all dependencies.

Zhou et al. (2021) further noted that PRAs conducted in these facilities also involve the challenges and problems in all domains relative to risk assessment and risk metrics involving multiunit sites.

Case Study: PRA and CI Risk

PRAs are essential in protecting CIs and understanding specific risks in homeland security. It also includes addressing risks related to social infrastructures deemed as critical and having interrelated interdependencies and network boundaries. For example, in one case study utilizing a PRA framework, Ongkowijoyo and Doloi found the domino effect can identify significant risks, threats, and vulnerabilities in "risk identification and risk assessment in electricity infrastructures" (p. 8) to mitigate challenges and problems.

Design and Methodology

Ongkowijoyo and Doloi (2017) suggested assessing probabilities using scientific methods that include "the failure mode effect and criticality analysis (FMECA), social network analysis (SNA), and fuzzy-set theory" (p. 5). These methods aim to analyze critical risks identified as the most critical "based on decision factors and risk impact propagation"

(Ongkowijoyo & Doloi, 2017, p. 5). Risk propagation refers to vulnerabilities and risks capable of causing disruptions in system networks and operational functions, fuzzy-set theories are mathematical computations used to examine uncertain sets, and stakeholder participation has membership functions. For example, a fuzzy-based critical risk analysis (FCRA) is conducted to illustrate the interrelated relationship between "stakeholder identification and hazard events identification" in PRA risk assessments (Ongkowijoyo & Doloi, 2017, p. 10).

Participants and Setting

In Ongkowijoyo and Doloi's (2017) research study, "stakeholders are referred to as persons, groups, or organizations" that participated in the study (p. 10). Participants and participation aim to mitigate risks and develop a comprehensive strategy for infrastructure designed to minimize and reduce the level of risk that can disrupt CIs and identify extreme hazardous events. A preliminary risk assessment is developed in the plan, designed in a long-term strategy to identify hazards, events, and risks, and includes stakeholder participation. In addition, the stakeholder participants work toward "embracing divergent perceptions" and conducting a "risk impact statement and propagation mechanism analysis" (Ongkowijoyo & Doloi, 2017, p. 9). The overall goal was to assess critical risks associated with urban infrastructure system risks by developing, integrating, and mitigating risk assessment methodologies.

Location and Purpose

The infrastructure risk assessment is performed organization-wide in an internal process. It does not involve identifying risks and vulnerabilities outside of the organizations or mitigating any external interdependent or interconnected organizations. The risk assessment includes a single system and does not include assessing risk outside of the organization or impacts to external organizations. Ongkowijoyo & Doloi (2017) research study aims to validate models based on a hypothetical case and apply empirical research that can contribute to future research. The practical and social implications are to provide an effective strategy in the decision-making process that will contribute to a seamless operation in society and increase CI and community resilience.

Findings

According to Ongkowijoyo and Doloi, research findings suggest that "fuzzy-based social network analysis (FSNA) methods" evaluate risks related to CIs and the community. Therefore, the FMECA methods and tools are essential in evaluating and ranking risks and providing a reasonable method to rank risks "based on their magnitude value within the traditional risk assessment method" (Ongkowijoyo & Doloi, 2017, p. 5). In addition, the probabilistic framework considers synergistic effects and noisy probabilities, can be used to evaluate common causes of failures, and can support decisions relevant to single risk evaluations; for example, when there is a lack of considering the domino effect in risk assessments and CI risks. According to Ongkowijoyo and Doloi (2017), this can impact the degrees of dependency placed on the community and identify uncertainty among various stakeholders and levels of perceptions in the decision-making process to mitigate risk and determine resilience and risk prevention processes.

Conclusion

In HLS, the concept borrows from other disciplines and theoretical perspectives to address the many needs of federal agencies within the DHS. According to Comiskey (2018), the field of HLS lacks a specific theory and framework, and DHS represents multiple fields of study and disciplines. The role of many federal agencies with DHS is to examine all probabilities, risks, and vulnerabilities to "prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risks to the Nation” (Comiskey, 2018, p. 29). In HLS, many of the theories used in the field are related to risk management, security theory, technology, and theories on terrorism and the radicalization process, leadership and management theories, critical theory, and probability theories (Comiskey, 2018). Considering all probabilities related to risk assessment and management in HLS requires developing a methodology for risk identification and assessment for CIs such as natural gas pipelines and electrical grid power systems’ critical infrastructures.

CHAPTER FOUR: FINDINGS

Overview

Chapter Four comprises PRA measures to mitigate high-rise buildings with potential mixed-use tenants (residential and commercial tenants). The research methodology consists of PRA and Bayesian networks and other measures. The research study also includes a framework for fire safety to preserve life and property. According to Tan et al. (2020), the framework can be applicable to HLS agencies and local fire departments in jurisdictions and geographical locations in a systematic approach "based on a comparative expected risk-to-life (ERL) methodology" (Tan. et al., 2). In addition, the research study provides an integrative quantitative framework in comprehensive risk models that address technical risk factors and factors related to safety and human life.

Design

The research design and theoretical perspectives presented in the research study related to PRAs have effectively understood how to mitigate risk in risk management and present a comprehensive quantitative research study. In the case study, according to Tan et al. (2020), PRAs are used as a methodology that "incorporates technical, human, and organizational risks" (T-H-O-Risk; p. 1); for example, in fire safety in a high-rise apartment building. An incremental approach to risk can increase and quantify the "impact of human and organizational errors" (HOEs) (Tan et al., 2020, p. 1) when fire safety involves different measures and fire safety systems when human and organizational factors (HOFs) are essential variables in assessing fire risk. Tan et al. explained that when assessing probabilities, the "Bayesian belief network" is a technique used to model human and organizational factors related to predictive modeling, and "human risk assessments" (HRAs) are factors related to human factors and risk (p. 3). THOR features include variations that evolve over a period of time and use system dynamics to model risk comparisons. For example, changes in building management behavior in high-rise buildings can create risk and risk to life variations and “expected risk to life due to technical, human, and organizational risk factors” (Tan et al., 2020, p. 1). In addition, Tan et al. noted that “80% of accidents” are caused by HOEs, and “fire safety designs that do not consider “human and organizational errors (HOEs) underestimate overall risk by approximately 20%” (p. 2). The term HOE is defined as characteristics that represent “collective departures from acceptable or desirable behavior by an individual or groups of individuals that may result in unacceptable or undesirable outcomes” (Tan et al., 2020, p. 2).

In high-rise buildings that house residents and critical infrastructure services and resources, fire systems are both active and passive emergency systems that can contribute to HOE and response to emergency incidents. An active system can include automatic fire suppression and detection systems such as sprinklers and fire alarms. Passive systems are designed to “suppress or slow the spread or contain fires and can include fire detectors, and smoke control systems” (Tan et al., 2020, p. 2). Tan et al. (2020) also suggested there is a probability of a mismatch between human and task-oriented functions during emergency incidents or in response to an emergency incident. Therefore, management staff and decision-makers can evaluate performance-shaping factors (PSFs) when after-action reports and other official reports are generated. The human error probability is calculated after the assessment and becomes a part of the risk assessment (p. 3). In the T-H-O-Risk methodology, designing building and performance metrics is an essential part of the process. It includes the deemed to satisfy (DtS) solutions, ensuring the design complies with standards and performance metrics, ensuring the relationship in each subsystem is tested and qualifies, and fire safety systems and preventive measures quantified in the F-N curve assessment. The framework ensures acceptability in the design pattern and addresses performance issues concerning fire safety systems.

Research Questions

RQ1

> RQ1: What is a theoretical approach to a probabilistic risk assessment (PRA) homeland security?

In HLS, fire departments, and critical infrastructure across the country, it is essential to "accurately estimate the value of probability in performing and not performing fire drills," especially when it involves CIs and high-rise buildings with a mixture of occupants (Tan et al., 2020, p. 2). Senior citizens often live on higher floors, and emergencies can hamper response times. In a scenario involving emergency response in high-rise buildings, considerations associated with several factors are relevant risks that can exceed an acceptable risk threshold. The T-H-O-Risk model in PRAs addresses the gaps necessary to quantify factors related to "technical, human, and organizational risks and uncertainties" (Tan et al., 2020, p. 25) related to risk probabilities in high-rise buildings. The methodological approach can also apply in other jurisdictions and geological locations. The Bayesian network incorporates HOEs and integrates SD modeling to make comparisons and account for variation in risks (Tan et al., 2020, p. 25). For each scenario related to a high-rise building in assessing probabilities, there is an event tree that illustrates five potential events that can occur as follows:

- The initial emergency event and response is called "fire yes-P(f)" (Tan et al., 2020, p. 6)
- Fires detected and "detection methods yes-P(d)" (p. 6)

- The ability to suppress fires is referred to as “fire suppression systems yes-P(Su)” (p. 6)
- Spread of fires and warning systems for building occupants—“warning system yes-P(BOWS)” (p. 6)
- High-rise buildings that have “egress protection systems” allow for “fire department response P(Fdr)” (p. 6)

In these types of scenarios, probabilities are the product of the emergency event as a “single event: P(Sc) = P(f)P(d)P(Su)P(SC)P(BOWS)P(Fdr)” (Tan et al., 2020, p. 6).

RQ2

RQ2: How are probabilistic risk assessments (PRA) applied in risk management? Probabilities uncertainty is a primary concern in risk management and should be viewed as a fundamental aspect of risk management assessment. An example is risk management in a fire scenario involving probabilities, in which the probability is P-1, and C1 represents consequences or the number of injuries or deaths resulting from Scenario-1. The *N* represents the number of scenarios where there is mitigation. Therefore, a risk definition of probability viewed from two perspectives are expected outcomes and risk as uncertainty, and a risk-based method will require an analysis of uncertainty. In this type of fire scenario, occupants of high-rise buildings are a priority, and risk management is an essential function in building management practices. In PRAs and risk management, HOEs, and SD, some variables are reliant on the “maintenance regime as a subsystem linked with other subsystems” (Tan et al., 2020, p. 8) in building management processes and organizational cultures. The SD model is a 2-step process, and the first step is the causal loop in the system comprised of causal relationships. These elements represent interactions in systems where feedback loops and delays in the time frame play an integral part. The second step is the “stock and flow diagram” (Tan et al., 2020, p. 8) and involves quantitative analysis. A stock is an entry flow that involves increasing “the value of a stock, and a flow exiting a stock decrease” over time (Tan et al., 2020, p. 6). The mathematical computation illustrated that the stocks and flows are related: “Stock =Z t 0 (Entry_ flow - Exit_ flow) dt” (Tan et al., 2020, p. 8).

RQ3

> RQ3: How are probabilistic risk assessments (PRAs) used to compare risk in critical infrastructures?

In the PRA, when comparing risk associated with fire safety and fire fatalities in CIs and high-rise residential buildings, data extrapolated in other countries such as Australia, Canada, New Zealand, and the UK indicate a range between “7.3 x 10 -6 to 1.3 x 10 x -5 deaths and year” (Tan et al., 2020, p. 17). When a high-rise residential building does not have active fire systems, the ERL is “1.68 x 10 - 3 to 8.38 x 10 - 3”; in a residential building that does not have an active system; the ERL is higher (Tan et al., 2020, p. 17). The T-H-O-Risk methodology and the ERL provide an alternative solution to make comparisons that are deemed to satisfy (DtS) with a solution integrated into the F-N framework and curves acceptable in the design. The F-N represents the frequency (F), and the (N) represents probabilities related to a cause or fatalities. The T-H-O-Risk methodological approach and ALARP principles contribute to comparative calculated risk values. The primary steps in the T-H-O-Risk methodological approach used in making comparisons involve data collection methods and analysis processes. These methods involve determining credible fire scenarios, performing risk assessments and scenario analysis, ranking risk and comparing fire scenarios, and performing a quantitative and qualitative risk analysis. In PRAs, comparing risks requires generating a fundamental equation in the first step, and the equation should highlight probabilities and consequences. Risk to occupants can be "calculated based on probable fire scenarios leading to the computation of ERL" (Tan et al., 2020, p. 9), and the ERL is compared to the HOE to determine the overall risk and compared to industry standards, according to Tan et al. (2020). Further, Tan et al. suggested the BN can provide data on calculated ignition frequencies and analyze global ERLs to understand the "dynamic effects of time-varying parameters effects of time-varying parameters" (p. 9).

According to Tan et al., in the research study, seven building designs were chosen in different geographical locations involving various climatic conditions to assess and compare HOE risk factors associated with residential high-rise fires. The study design focused on "active fire safety systems in high-rise residential buildings" (p. 25) and to determine the best approach to fire safety systems and understand the impact of HOEs on sprinklers systems, smoke detectors, "building occupant warning systems (BOWS), and smoke control systems" (Tan et al., 2020, p. 25). In addition, a focus is also placed on building risk level benchmarks, assessing human and organizational errors, and determining if the specific factors exceed the threshold for acceptable risk. Key assumptions introduced were based on risk estimations, calculations, and design perimeters based on probability and an estimation of the potential consequences.

Hypotheses

The null hypotheses for this study are relevant to the research questions listed below:

RQ1: What is a theoretical approach to a probabilistic risk assessment (PRA) homeland security?

$H_0$1: In CIs and homeland security, PRAs and the T-H-O-Risk methodology can be essential for emergency response plans and training.

According to Tan et al. (2020), in a theoretical approach to risk assessments that includes a PRA, the T-H-O-Risk methodology can be applied in other jurisdictions if the HOE utilizes the BN and sees risk variations in SD modeling. For example, in SD mapping, nonlinear factors can impact BN and the HOE variables in data analysis. It can include deficiencies in training, inefficient emergency plans, non-compliance with standards, no check rules, deficiencies in maintenance procedures, incorrect risk assessment, not following predetermined standards, and an improper safety organizational structure.

According to Huse (2018), in HLS, as well as critical infrastructures and building structures, targeted violence and public safety are a significant concern for HLS agencies and law enforcement because of the probabilities associated with "single-attacker events, whether assassinations, school shootings, or lone-wolf terrorist attacks" (p. 17). In some cases, agencies use registered probabilities to analyze hypothetical scenarios in super-forecasting. In the case of super-forecasting, in the process, a group engages in analytical processes to evaluate threats "compared to a single-agency method" (Huse, 2018, p. 17). Probabilities receive scores according to the level of binary accuracy based on whether occurrence did or did not occur. For example, suppose a forecaster ranks a 75% probability of an event occurring. In that case, the forecaster will receive a higher score than a forecaster who ranked an outcome of 60% probability outcome. Huse's hypothesis suggests that ranking probabilities using a super-forecasting methodological approach will provide a "more thorough, accurate, and predictive analysis than a single organization" (p. 41). In super-forecasting acts of targeted violence involving critical infrastructure, there is a probability of "inherent institutional and cognitive vulnerabilities" due to inadequate data and information and failure to properly investigate and detect probabilities of an event within a single organization (Huse, 2018, p. 42). Data sources are used to conduct quantitative statistical analysis for super-forecasting probabilities concerning targeted violence and lone actor attacks; research sources will include publicly available data. Information can be obtained from unclassified sources such as the "START Global Terrorism Database" and data compiled from case studies to create a scored and analyzed synopsis (Huse, 2018, p. 42).

RQ2: How are probabilistic risk assessments (PRA) applied in risk management?

$H_0$2: In risk management, CIs, and homeland security, a quantitative analysis is essential in addressing HOE and understanding the role of PRAs to protect infrastructure from failures and domestic threats and provide safety in high-rise buildings.

According to Tan et al., in PRAs and risk management, human and organizational errors (HOE) are significant when addressing the complexity of the fire system. For example, the expected risk-to-life (ERL) can influence safety provisions, leading to a 33% increase with a more straightforward design, and a new sprinkler system can lead to a "+20 increase in the ERL" (Tan et al., 2020, p. 25). In PRAs, building design can involve different human characteristics and organizational scenarios, designs, and organizational standards such as maintenance procedures, safety systems, and emergency planning. In some cases, there can be a positive correlation between the ratio in HOE and ERL based on the number of active systems, and values in HOE may "range from 8–13% and increase to 25–38% when all four active systems are present in the trial design" (Tan et al., 2020, p. 25).

According to Valentin Torres (2020), the BN theoretical approach can be instrumental in making predictions, management decisions, risk evaluations, and strategic planning in risk management. In addition, the approach can also help predict casual relationships in BN risk evaluations and “improve network performance” (Valentin Torres, 2020, p. 4). In assessing probabilities, a fault tree analysis (FTA) is referred to as a visual approach designed to “break down the failure of a system into source events trees using event and gate symbols to structure cause and effect relationships of a failure” (Valentin Torres, 2020, p. 20). An FTA is a technique used to reflect a logical sequence to failures or the probability of failure.

In addition, according to Valentin Torres (2020), malicious software can exploit critical infrastructure and network devices and require a fundamental framework designed to provide adequate cyber-security to prevent CIs from becoming infected, damaged, disruptions, and suffering a loss of control systems. In one hypothesis presented by Valentin Torres, a correlated analysis of system networks in risk management suggests probabilities and predictions are reliant on network performance status. Valentin Torres suggested network risk occurrences and how challenges are “correlated to the network performance is reliant on performance values with less than 0.5 with a confidence interval of 95% and *p*-value less than 0.05” (p. 66). For example, calculating probability in an FTA can be calculated based on the output event if an event applies to the analysis. The FTA calculation and results can also include factors related to Poisson density function (PDF), gamma Poisson distribution (GPD), and generalized linear model (GLM) to help determine the impact network risk incidents can have on performance to achieve a “confidence interval of 95% and p-value less than 0.05” (Valentin Torres, 2020, p. 66). According to Valentin Torres, “correlation analyses do not predict the likelihood of network performance and do not show significant evidence to reject the null hypotheses, because of the confidence interval of 95% and p-value less than 0.05” (p. 67).

RQ3: How are probabilistic risk assessments (PRA) used to compare risk in critical infrastructures?

H_03: In risk management, PRAs and quantitative analysis are essential in comparative analysis related to pipeline safety and assessing electrical power grid systems and power stations.

According to Karki (2020), in protecting CIs such as natural gas pipelines and electric power grid systems, risk management is a process that involves future assessment to protect these resources from failure and domestic terrorists by creating better design, construction, and preventive measures. With CI risk assessment, a quantitative analysis is performed on system functions to calculate and compare differences in factors related to the pipeline's age. An example is two different scores compared to determine the differences in number scores to determine if "the pipeline is older or more recent in age" (Karki, 2020, p. 11). In conducting a risk assessment on pipeline crossings, a risk analysis tool follows "Guidelines for Utility Encasement Policy for Highway Crossings" (Karki, 2020, p. 24). The process provides a comparative corrosion analysis using the casing corrosion direct assessment (CCDA). In conducting risk assessments, a second process includes "a general system of relative risk scores" (RRS; Karki, 2020, p. 11). The goal is to categorize probable pipeline failures. For example, to determine the null hypothesis related to "the output of the average nearest neighbor tool," the process includes observing the "mean distance and expected mean difference, nearest neighbor ratio, z-score, and *p*-value" (Karki, 2020, p. 40). The *z* score and *p* value can help determine if the null hypothesis is rejected and if the rejection is related to the means if the *z* score and *p* value are not part of the data set and the data set is not part of a random pattern. According to Karki, conducting a risk assessment on probability can help determine if "a random process creates the observed spatial pattern" (p. 41) when the probability consider as a small *p*-value output, according to Karki (p. 41). Scripture teaches, "according to all that I am to show you, the pattern of the tabernacle and the pattern of all its furniture so that you can construct it" (*King James Bible*, 1769/2021, Exodus 25:9).

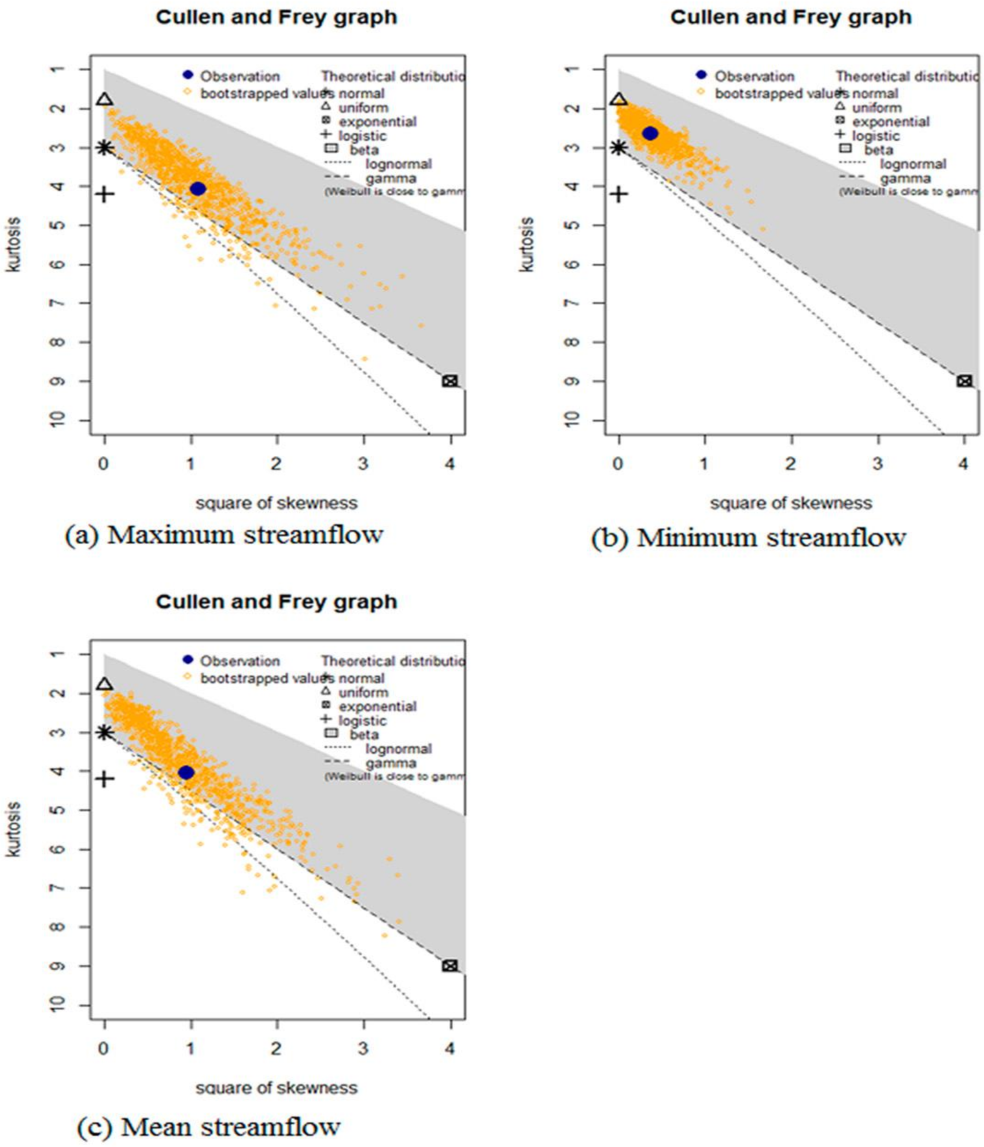
Descriptive Statistics

According to Langat et al. (2019), studies involving hydrological environments utilize descriptive statistics applicable in designing models, organizational planning, and managing water systems, critical infrastructures, and ecosystems. In these studies, probability distribution models are used to conduct analysis. Depending on the choice of model and the frequency analysis, critical analysis can include "an event-descriptive variable" and a distribution model to assess historical data (Langat et al., 2019, p. 2). In some cases, a distribution model can include a "best-fit probability distribution" (Langat et al., 2019, p. 2) and perimeters that estimate certain factors. In classical descriptive statistics, a prerequisite can include probability distribution and determining the type of analysis.

Langat et al. (2019) noted an example is the water distribution systems, where descriptive statistics can include factors relative to "maximum streamflow, minimum streamflow, and mean streamflow" (p. 9). Datasets provided through streamflow datasets are used to conduct an "extreme flood analysis, contribute to drought investigations, reservoir volumes studies, and time-series modeling (Langat et al., 2019, p. 9). In quantitative research, descriptive statistics summarize specific datasets or samples represented by a variable mean, standard deviation, or frequency level and are used to understand elements of a dataset or collective properties. In some cases, a distribution with specific graphical functions illustrates the goodness of fit. To plot a graphical representation and visualization of the goodness of fit, quantile–quantile (Q–Q) plots construct a graphical assessment and visualization of the goodness of fit. In descriptive statistics, a probability-probability (P–P) plot is a simple way to construct a graphical procedure that assesses a “forecast prediction and assesses the forecast uncertainty” based on probability values (Langat et al., 2019, p. 13). For example, Figure 2 illustrates a “normal distribution with uncertainty or skewness and kurtosis estimated by bootstrap” that illustrates extreme floods (Langat et al., 2019, p. 11).

Figure 4

Cullen and Frey Graphs Showing Streamflow



(a) Maximum streamflow

(b) Minimum streamflow

(c) Mean streamflow

In CI water distribution systems, the best-fit-model probability distributions and the null hypothesis testing based on the minimum Akaike information criterion (AIC) value calculated and the Bayesian information criterion (BIC), according to Langat et al. (2019, p. 9).

According to Che-Castaldo et al. (2021), an electric power grid system is considered an essential resource in society that connects multiple infrastructures. Other CIs are also interconnected through the power grid system. Across critical risk indicator (CRI) domains, there is a diverse number of CIs and these power grid systems are guided by "human activity and public policy" in terms of supply and demand (Che-Castaldo et al., 2021, p. 594). Che-Castaldo et al. noted that electric power grid systems are emerging as a class of human and natural systems that involve complexity and independence. The primary function and processes are controlled through computers and communication network systems. Descriptive statistics illustrate the System Average Interruption Duration Index (SAIDI) in electric power grid systems. This data process uses "metrics to quantify disturbances on the power grid" (Che-Castaldo et al., 2021, p. 608).

The IEEE Guide for Electric Power Distribution Reliability Indices also employs metrics to quantify the average amount of time customers are without power or the amount of time for system disruptions. According to Che-Castaldo et al., risk measures that involve probabilities aim to focus on measures such as systemic risk measures: marginal expected shortfall (MES), SRISK, turbulence measures, and network connectedness methods" that can include statistics to highlight processes and to capture "systemic risk in human and natural systems" (p. 612). In addition, measures related to descriptive statistics can also include variables associated with stakeholders, stockholders, reservoir operators, CIs, civil infrastructure streamflow, and monitoring future risk and monthly outlook distribution datasets based on raw data, according to

Che-Castaldo et al. Scripture teaches “Who has measured the waters in the hollow of his hand, or with the breadth of his hand and meted out heaven with the span, and comprehended the dust of the earth in a measure, and weighed the mountains in scales, and the hill in a balance” in (*King James Bible*, 1769/2021, Isaiah 40:12).

Results

$\mathbf{H_0 1}$

According to Huse (2018), in the decision-making process, simulations contribute to an awareness of threat assessments and provide a 2-part survey highlighting the strengths in threat assessments, identifying uncertainties and what is statistically unpredictable, and providing a multidisciplinary method to conduct analysis. In viewing five scenarios relevant to targeted violence, hypothesis testing involves Monto Carlo methods in a time series autocorrelation analysis to conduct tests. The aim was to conduct tests involving pattern detection to determine if specific patterns emerge and justify any rejection of the hypothesis concerning lone wolf actors’ targeted violence over time to determine randomness. Huse noted no correlation in statistical testing in the hypothesis generated by the scenarios, and there were “weak correlations noted between latitude data and lags of t-1 and t-2” (Huse, 2018, pp. 82–83). A quantitative analysis of violent attack data includes an experimental survey, and the super-forecasting methodological approach uses a Brier score evaluation information. Information suggests “the hypothesis that the networked interagency analysts produce results that are significantly different from investigative agencies,” and the survey instrument produced output data for the analysis to help determine how analysts reach decisions (Huse, 2018, p. 20)

$H_0$2

According to Valentin Torres (2020), in conducting quantitative research, the multiple logistic regression (MLR) results suggest that probabilities and predictive modeling can help predict the impact of network performance. In some situations, the MLR and network performance can affect the “current status, customer impact, and network failure related to network risk incidents” (Valentin Torres, 2020, p. 72). For example, it can lead to the likelihood of failure for a source of impact when there is “a 95% confidence interval and a *p* value less than 0.05” (Valentin Torres, 2020, p. 72). Therefore, according to Valentin Torres, the results suggest there was no reason or evidence to reject the third null hypothesis. The reason was that the “confidence interval of 95% and a *p* value less than 0.05” (Valentin Torres, 2020, p. 68) and there was no likelihood of failure in network performance. In addition, a descriptive analysis establishes the “minimum, maximum, mean, standard deviation, and variance of the independent and dependent variables” to determine six independent variables in network performance (Valentin Torres, 2020, p. 36).

$H_0$3

According to Karki (2020), the author asserts that the null hypothesis is directed toward analyzing patterns in the toolset to determine spatial randomness in data. To determine if there is probability in *p* values observed in spatial patterns and to illustrate when there is a small amount of probability in *p* values. The spatial statistics were calculated before the confidence level was obtained based on a 99% confidence level to represent a conservative case to reject the null hypothesis. Statistical data can be retrieved from the global information system (GIS) to focus on mapmaking and comparison of data, “data analysis, and statistical analysis,” according to Karki (p. 45). The goal is to understand probabilities and uncertainties and conduct a “risk analysis of pipeline, characteristics of pipeline failure," the importance of the age factor in pipeline failures, and the significance of "GIS spatial analysis and methods to improve pipeline design and regulations" (Karki, 2020, p. 45). Scripture teaches, "It is the Glory of God to conceal a thing, but the honor of kings is to search out a matter" (King James Bible, 1769/2021, Proverbs 25:2).

CHAPTER FIVE: CONCLUSION

Overview

The purpose of Chapter Five is to provide a clear interpretation of probabilistic risk assessments (PRAs) in critical infrastructure (CI) and homeland security and express the importance of considering PRAs in addressing issues, problems, and uncertainties associated with risk and threats as well as in providing protective measures for infrastructures. The chapter also includes the overall context of the research and the significance of research findings.

Discussion

The research methodology utilized PRAs, Bayesian networks, and other concepts. The aim of this research study was to provide a PRA framework for fire safety to preserve life and property and mitigate human and organizational errors (HOEs) and threats posed by domestic terrorists and violent extremists. These factors play a significant role when assessing PRAs to protect human life, critical infrastructure, and homeland security elements. According to Suave and Van Acker (2021), when modeling uncertainties in PRAs, a life cycle assessment may be conducted. The goal is to address uncertainties, vulnerabilities, and risks when there is a lack of or limited knowledge about a system and inherent consideration given to spatial and temporal variability in the stochastic process. In some instances, an assessment can require an "integrated life cycle assessment (LCA) and quantitative risk assessment (QRA)" (Suave & Van Acker, 2021, p. 591). For example, to understand the likelihood of an event, crisis, occurrence, and consequences, the process can include integrating tools and developing a framework design to provide probability estimates weighed in various scenarios to improve the overall spatial and temporal factors. The process can also include developing an event tree design to provide the basis to understand the probability of occurrence in each scenario. According to Suave and Van

Acker, test applicability will require computing all values and standard deviations in each scenario to determine if the impact is related to cumulative probability. These factors will help determine if the PRA data and information obtained from existing conditions can have future implications.

According to Glette-Iversen et al. (2022), in a comparative view of quantitative risk analysis and assessments, plausibility is considered an example of uncertainty similar to probability in meaning. The concept is also referred to when analyzing a scenario when there is an emerging risk. On the other hand, plausibility is considered a tool for measuring uncertainty in a qualitative approach, but risk and uncertainty must be clarified. Another definition of probability is incomplete knowledge, limits that lack accuracy, and an assumption that is misleading and lacks transparency. On the other hand, a suitable term for probabilities is the term that can be defined as a subjective judgment or subjective probability and the likelihood of risk. A significant factor in distinguishing the difference between plausibility and probability is applying the terms in scenarios and forecasts. It depends on how risks are characterized according to feasibility or plausibility versus the likelihood of an occurrence. Glette-Iversen et al. suggest that if probabilities cannot be used to quantify or measure a scenario, a body of evidence may be used to measure outcomes in “terms of plausibility or convincingness of the evidence” (p. 6). In addition, the Dempster-Shafer theory (DST) provides a generalization of the Bayesian theoretical perspective that represents subjective probability, which suggests probability is a belief function and features of plausibility provide measures of uncertainty. The DST is also considered an evidence theory, and it is a theoretical approach that focuses on reasoning with elements of uncertainty through evidence. The Scripture teaches, as evidenced in the Bible, “All Scripture is given by inspiration of God, and is profitable for doctrine, for reproof, for correction, and for instruction in righteousness that the man of God may be thoroughly furnished onto all good works" (*King James Bible*, 1769/2021, 2 Timothy 3:16-17).

According to Zio et al. (2022), in probabilistic risk assessments, the Bayesian belief network is a graphical model designed to provide data to represent conditions related to dependencies and random variables. Through the model, probabilities are quantified based on a set of nodes and propagated evidence gathered from network elements. Furthermore, the network is designed to model systems complexities and include multiple scenarios, and the inference may be listed as forward, backward, or intercausal formation. In some instances, joint computing probabilities can involve estimating marginal probabilities, and setting perimeters can include "examining the maximum likelihood" (Zio et al., 2022, p. 6). Elicitation can require an expert in a specific field, and through an expert, conditional probabilities information obtained may provide recorded data, analytical design, framework, and perimeters; missing data concerning the conditions and the environment, and preliminary testing.

In some cases, an expert compiles marginal and conditional probabilities using a probability scale and in conditional probability table (CPT) highlighting the states of different nodes. In some case studies, the quantitative part of a conditional probability table requires the Bayesian Belief Network (BBN) to assign probabilities and perimeters. Additional time may require calibrating the weights to target specific probabilities. In some cases, the aim may be to reduce probability uncertainties that may require reassessing probabilities to determine levels of uncertainty.

Research Questions

RQ1

RQ1: What is a theoretical approach to a probabilistic risk assessment (PRA) in homeland security?

According to Cheng et al. (2022), probability methods such as Bayesian networks, stochastic theories, and resiliency are essential in homeland security. Assessing the performance of CIs is vital to ensure the normal operations of systems and networks that are interconnected and interdependent. Cheng et al. suggest maintaining resiliency and minimizing hazards require a framework to address all-hazards systems face and countermeasures to mitigate hazards. To quantify hazards in some instances will involve a subject matter expert (SME) for the "construction of probability distributions and risk calculations" to develop resiliency metrics (Cheng et al., 2022, p. 596). In homeland security, metrics for CIs can include factors relative to the "probability of performance recovery" (Cheng et al., 2022, p. 598). In the approach, the goal is to focus on the system's ability to absorb hazards and resume normal operations, redundant functions, and resources to recover from hazards and system failures.

PRAs will also include metrics to assess performance recovery time. Depending on the CI target to protect the recovery process will involve a stochastic process. The main goal is to ensure an available recovery source and assess the hazard's severity and occurrence based on probabilities. In CIs, probabilistic metrics can specifically include the following:

- The probability performance function is restored to normal functions within a level period.
- Reliability will complement probable failure.
- Performance and recovery must meet specific thresholds.

- Conditional probability must ensure performance recovery will be within a level period.
- Multiple indicators will be assessed based on the “sum of reliability and recovery ability” (Cheng et al., 2022, p. 599).

CI resiliency and PRAs can be formulated conceptually, qualitatively, and quantitatively in research studies to address elements of resiliency and, in a general or specific context, to address the needs of CIs, community resilience, and engineering resilience.

RQ2

RQ2: How are probabilistic risk assessments (PRA) applied in risk management?

According to Silva et al. (2021), in risk management, evaluating risk a PRA can involve Bayesian theorem, Monte Carlo simulation, and other analytical processes that evaluate and identify risk and occurrences that have probable consequences and negative consequences connotations. In some elements of risk management, it is the belief that the impact of risk and probabilities are independent. Risk management in some supply chains believes risks are a cascading effect and observe risk to mitigate the problem. Silva et al. suggest that in measuring risks, conditional factors should be incorporated, and the probability of the occurrence must be calculated conditionally. Measuring risk involves two components: (a) the probability of an event and occurrence and (b) the assessed consequences and the impact of the risk. Silva et al. suggested that some managers are not comfortable with probability estimates in supply chains. In other situations, managers of companies’ data are not available or scarce and are unaware of how to “estimate the variables through subjective judgments” (Silva et al., 2021, p. 2962).

According to Winterfeldt et al. (2020), a risk-informed benefit-cost analysis (BCA) is necessary for homeland security in risk management. Tools applicable in risk management are designed to integrate functions related to analyzing risks, making decisions, and examining a BCA. In risk management, probability and consequences are measured by objective decision-makers to model value, and outcomes can be based on a specific scenario. In addition, these factors can also be reliant on an alternate case to produce specific results. In some situations, a BCA can retain probability and consequences as a driver for change and make critical decisions and tradeoffs according to estimates and valuations. In some elements of homeland security, the decision-making process for detecting threats and improving threat detection will involve threat probability, assessing the threat landscape, baseline reductions, and detection probability. The process can also include implementing programs that will help to reduce false alarms and contribute to an increase in detection measures or counterterrorism efforts. In modeling probability, an assessment can include analyzing uncertainties and consequences. The PRA analysis process can include one variable at a time and model “probability distributions of net benefits calculated using standard probabilistic simulation software” (Winterfeldt et al., 2020, p. 460).

RQ3

> RQ3: How are probabilistic risk assessments (PRAs) used to compare risk in critical infrastructures?

According to Chatterjee et al. (2021), in homeland security and CIs, an analysis is conducted to identify risks, threats, and vulnerabilities when comparing risks. Critical systems are analyzed to determine how hazards, threats, and vulnerabilities evolve. In PRAs, comparisons can include incorporating strategies and risk assessments to update data from SMEs. To compare PRAs in CIs, the risk management staff determines if the analysis will include qualitative, semiquantitative, or quantitative methods and adopt probabilistic assessments and various theoretical perspectives. In HLS, to meet the security challenges to protect CIs can require comparisons and editing of PRA methods to meet the challenges to provide "new applications of security risk analysis methods" (Chatterjee et al., 2021, p. xxvi). In some cases, in managing CIs, preventive measures can be compared to allocated resources to reduce the probability of disruptions, system failures, preparation, and the consequences associated with an event.

According to Flage et al. (2018), making a comparison between a "probability bounds analysis and a subjective probability" would involve assessing epistemic uncertainties to help determine unknown perimeters in probability models (p. 1). The process can include a subjective probability approach and developing a probability structure to illustrate and quantify uncertainties or a modeled set of perimeters. An essential criticism is that subjective probability distributions are based on unjustified assumptions if data and information are insufficient and no proper analysis is conducted. A probability bounds analysis (PBA) is a process that is considered a "marriage between probability theory and interval analysis" (Flage et al., 2018, p. 2), and deviation in assessments uncertainties can be related to (a) distribution patterns and perimeters, (b) the shape of the distribution, (c) the interconnectedness of the variable dependence, and (d) the model of the structure. There are two approaches to making probability comparisons. The first, subjective probability, involves a crude assessment, perimeter estimates are modeled, and the model uses perimeter distributions. The second approach is a PBA, which requires detailed assessments in both stages. In comparison, assumptions are a part of risk assessments and should be given attention in the "assessment phase and the follow-up phase" (Flage et al., 2018, p. 9).

In conflicting views on PRAs in large infrastructures, Oliva et al. (2021) suggested that risk assessment can help guide construction sites but requires an estimation of probabilities to assess the likelihood of an event and when an event is likely to occur. In some cases, this can be difficult because of limited knowledge about an attacker, and there may be limited historical and reliable data. Some situations will require SMEs to meet with security personnel, risk management staff, and members of academia, industry, and local law enforcement to compare and contrast a “multi-criteria decision model” (Oliva et al., 2021, p. 1).

Implications

In viewing future implications of measuring probabilities and uncertainties, according to Logan et al. (2021), the Society of Risk Analysis’s glossary characterizes risk as consequences and uncertainties involving an event, hazard, damage, and vulnerabilities that exist related to activity and can be measured by probabilities. In PRAs and risk assessment, the implications are in understanding the “choice of the temporal intervals for observing the activity” (Logan et al., 2021, p. 1967) and considering the consequences. In managing risk in HLS and CIs, Logan et al. suggested the implications are far-reaching; for example, how to effectively manage community risk and communicate through a framework where there is intergenerational decision-making and how to function under specific circumstances and conditions to assess risk uncertainties and provide adequate protective and preventive measures. Other implications relate to reducing risks for future generations and encouraging risk reduction in future generations to mitigate threats and vulnerabilities and emerging uncertainties in society relative to human life and CIs and HLS.

According to Fjaeran and Aven (2021), the social amplification of risk framework (SARF) is a process used to compare traditional methods of risk assessments from an “uncertainty-based risk perspective” to support assigned probabilities (Fjaeran & Aven, 2021, p. 673). In this process, PRAs identify problems according to their complexity, level of uncertainty, and whether or not there are conflicting values. In addition, the implications of risks can include both the attenuation and amplification process, and PRAs can be conducted to avoid an "uncertainty-based understanding of risk that prevents attenuation in risk assessment and management" (Fjaeran & Aven, 2021, p. 675).

Limitations

According to Winterfeldt et al. (2020), limitations are often consistent with views on lessons learned from the most recent model and the details offered through a risk value model about data and parametric assumptions and comparisons with an existing model. Winterfeldt et al. stated that the most challenging part of the deterrence process is deterring threats to CIs and HLS because of the "complex behavioral response between the defender's actions and the attacker's response" (p. 472). In some cases, limitations are placed on research products and in measuring probabilities, and the most significant "uncertainty comes from the variables that influenced the success of implementation, and in some cases from the variables that characterized unintended consequences of the implementation" (Winterfeldt et al., 2020, p. 473). In HLS agencies, PRAs and lessons learned to address uncertainties can contribute to existing and future applications.

According to Suo et al. (2021), research studies have highlighted the importance of CI risk factors and provided PRA models for CIs and data sources that help reference specific historical data and information for CIs. However, there are limitations related to the following:

- The vast multiplicity of risk factors,
- The interdependencies among some CIs,
- CIs that lack dynamic stochasticity, and
- CIs that lack multisource data can pose a challenge in quantifying problems associated with CIs.

Sou et al. noted that their research study’s primary purpose was to help develop a model to help overcome limitations and reduce barriers by acquiring additional information through data and information obtained from sampling, text mining, statistical, and simulation tools on expert subjective judgment. Suo et al. suggested that to help overcome internal and external challenges and limitations, factors to be considered in an effective PRA model should integrate multisource data and conduct multidimensional analysis from data collected from PRA scenarios. Therefore, the model includes “scenario elements, scenario evolution, and scenario effects” in a dynamic stochastic probability model (Suo et al., 2021, p. 2).

According to Ongkowijoyo and Doloi (2017), in homeland security, another model can consist of the domino effect integrated into a probabilistic framework that considers factors such as synergistic effects of risk, noisy probabilities, and assessing the common causes of failures. Ongkowijoyo and Doloi stated that risk assessments in CIs require an organization-wide approach and involve risks that impact the organization and the potential impacts of interconnected external organizations. Traditional risk assessments involve specific risks within the scope of the community, and conventional risk assessments are more directed toward security threats outside the normal scope of threats that can impact society as a whole based on a specific analysis, according to Ongkowijoyo and Doloi.

Conclusion and Recommendations for Future Research

According to Aven (2008), PRAs and probability should not be viewed as a perfect tool to address uncertainty, but knowing how to measure probabilities is advisable. Knowing the basic tenets of probability, theoretical perspectives, and statistical analysis is also advisable. Probability dimensions in a description of risk are viewed as

- Probability versus consequences measured on four levels,

- The high probability is 50%,
- The probability is 10 to 50%,
- The unlikeliness is negative at 2%.

The risk matrix can be set up to identify various risk categories and probabilities and risk descriptions and identify the main safety functions

- To prevent escalation of an event or threat,
- To maintain load barring specifications based on probabilities,
- To protect the environment and to prevent accidental events;
- To protect CI and HLS facilities in safe areas from attackers, predators, and imminent danger or threats;
- To conduct PRAs on "evacuation, facility safe areas, and safety personnel rescue" (Aven, 2008, p. 26).

The risk matrix today is supported by more sophisticated methods for risk assessments.

In PRAs today, new models have been created to provide more advanced methods to conduct risk assessments; these categories are essential to provide adequate protection and preventive measures for CIs and HLS governed by public policy and new standards. According to Picoco et al. (2020), to meet the future demands for PRAs, robust computational tools and advanced technological resources have led to improvements in "dynamic methodologies for the probabilistic risk assessment (PRA) of nuclear power plants" (p. 1). Tradition methods in PRAs involved the event tree method, and today the safety of CIs and elements of HLS involves "dynamic probabilistic risk and safety assessment (DPRA/DPSA) methodologies" (Picoco et al., 2020, p. 1). DPRA models are integrated with probabilistic perspectives to fashion systems and networks related to aleatory events, uncertainties, system failures, system recoveries, and other challenges and problems. To be used in future PRAs are

- The thermal-hydraulic model in PRAs provides perimeters for reactor design to support plant efficiency and the cooling ability in systems and assess “arbitrary time intervals” (Picoco et al., 2020, p. 6).
- A DPRA is used in accident scenarios, and simulations provide a large amount of data, are observed visually, and involve DPRA analysis and framework.
- A dynamic event tree (DET) is “viewed as a combination of PRA methods with deterministic and thermal-hydraulic (TH) studies” (Picoco et al., 2020, p. 2). The DET is also applicable in PRA methods, peer-review studies, and quality assurance.
- Statecharts are used to check the “Unified Modeling Language (UML) language” (Picoco et al., 2020, p. 2).
- The YAKINDU State Chart Tools (YSCT) is a verification strategy to help develop a graphical representation of the state chart.
- In PRAs, the graphical model provides a view and visualization of the simulator so the analyst can understand how processes evolve.

In many of the models used in these applications, the aim is to provide the analyst with sufficient knowledge of how systems perform, observe the appropriate system behavior, and understand the uncertainties, “whether safety systems for mitigation will operate or not, and quantify the likelihood of an occurrence. Scripture teaches, “The Lord shall fight for you, and ye shall hold your peace” (King James Bible, 1769/2021, Exodus 14:14).

The Homeland Security Affairs (HAS) (2020) suggests in an article titled, “Enhancing the Organization of the United States Department of Homeland Security to Account for National

Risk" (HAS, p. 1). To be effective in homeland security and national security requires a proactive approach nationwide to allocate and relocate resources, ensure resources provide the best support to mitigate risks, take an all-hazard to the nation's challenges and problems, and prioritize risk related to CIs and HLS. In addition, to be effective, the DHS must realign resources and promote networking among stakeholders in an effort designed to enhance organizational structures in DHS mission areas. Finally, it will require assessing risks and categorizing hazards. The risk methodology should include identifying risk as a function related to "threats, vulnerabilities, and consequences (Risk = F (T, V, C)" (HSA, 2020, p. 2). In addressing external and domestic terrorism elements in the U.S., which are far more complex, probabilities and consequences must be rooted in historical data from past experiences, which can require multiple approaches to deal with the complexities. Theoretical perspectives and models can also include

- Agent-based models
- Bayesian belief networks
- Bayesian event trees
- Decision trees
- Fault trees
- Game theory

In conducting probabilistic risk assessments in HLS, the future implications should consider the drivers for change and a "historical-trends analysis to determine future requirements" (HAS, 2020, p. 10). Scripture teaches, "I know the plans, I have for you, declares the Lord, plans to prosper you, and not to harm you and plans to give you a hope and a future" (*King James Bible*, 1769/2021, Jeremiah 29:11).

REFERENCES

Anthony, F. V., & Hermans, C. A. M. (2020). Spiritual determinants and situational contingencies of transformational leadership. *Acta Theologica, 40,* 60–85. https://doi.org/10.18820/23099089/actat.Sup30.3

Baggott, S. S., & Santos, J. R. (2020). A risk analysis framework for cyber security and critical infrastructure protection of the U.S. electric power grid. *Risk Analysis*, *40*(9), 1744–1761. https://doi.org/10.1111/risa.13511

Bellavita, C. (2019, September). How to learn about homeland security. *Homeland Security Affairs*, *15*(5). https://www.hsaj.org/articles/15395

Beyza, J., Garcia-Paricio, E., & Yusta, J. M. (2019). Applying complex network theory to the vulnerability assessment of interdependent energy infrastructures. *Energies*, *12*(3), 421. https://doi.org/10.3390/en12030421

Comiskey, J. (2018). Theory for homeland security. *Journal of Homeland Security Education*, *7*, 29–45. https://jsire.org/theory-for-homeland-security/

Danko, T. (2019). Student perceptions in homeland security and emergency management education: Experiential learning survey. *Journal of Experiential Education*, *42*(4), 417–427. https://doi.org/10.1177%2F1053825919873678

Davis, A. P., & Zhang, Y. (2019). Civil society and exposure to domestic terrorist attacks: Evidence from a cross-national quantitative analysis, 1970–2010. *International Journal of Comparative Sociology*, *60*(3), 173–189. https://doi.org/10.1177/0020715219837752

Davis, P. (2019). The threat of domestic terrorism: Combating targeted violence. *Journal of Counterterrorism & Homeland Security International*, *25*(2), 10–12. https://web-a-ebscohost-com.ezproxy.liberty.edu/ehost/pdfviewer/pdfviewer?vid=12&sid=ad1758dd-87e5-428b-9447-57f77a5c0899%40sessionmgr4008

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review, 26*(1), 69–75. https://doi.org/10.2478/raft-2021-0011

Deka, D., & Fei, D. (2019). A comparison of the personal and neighborhood characteristics associated with ride-sourcing, transit use, and driving with NHTS data. *Journal of Transport Geography, 76*, 24–33. https://doi.org/10.1016/j.jtrangeo.2019.03.001

Dick, K., Russell, L., Souley Dosso, Y., Kwamena, F., & Green, J. R. (2019). Deep learning for critical infrastructure resilience. *Journal of Infrastructure Systems, 25*(2), 5019003. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000477

Forman, P. J. (2020). Security and the subsurface: Natural gas and the visualization of possibility spaces. *Geopolitics, 25*(1), 143–166. https://doi.org/10.1080/14650045.2018.1513918

Grady, C., Rajtmajer, S., & Dennis, L. (2021). When intelligent systems fail: The ethics of cyber-physical critical infrastructure risk. *IEEE Transactions on Technology and Society, 2*(1), 6–14. https://doi.org/10.1109/TTS.2021.3058605

Haase, T. W., & Demiroz, F. (2020). Considerations of resilience in the homeland security literature: Towards conceptual convergence? *Journal of Homeland Security & Emergency Management*, *17*(2), 1–13. https://doi-org.ezproxy.liberty.edu/10.1515/jhsem-2018-0078

Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2021). *Introduction to emergency management* (Chapter 9, p.p. 410-414 (7th ed.). Elsevier. https://ebookcentral-proquest-com.ezproxy.liberty.edu/lib/liberty/detail.action?pq-origsite=summon&docID=534876

Heyerdahl, A. (2021). Risk assessment without the risk? A controversy about security and risk in Norway. *Journal of Risk Research*. https://doi.org/10.1080/13669877.2021.1936610

Kampova, K., Lovecek, T., & Rehak, D. (2020). Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. *International Journal of Critical Infrastructure Protection, 30*, 100376. https://doi.org/10.1016/j.ijcip.2020.100376

King James Bible. (2021). King James Bible Online. https://www.kingjamesbibleonline.org/ (Original work published 1769)

Korstanje, M. E. (2021). Tracing the cultural background of lone-wolf terrorism: Dilemmas, contradictions, and opportunities for the next decade. *International Journal of Cyber Warfare and Terrorism (IJCWT), 11*(1), 45–56. https://www.igi-global.com/article/tracing-the-cultural-background-of-lone-wolf-terrorism/270456

Kumar, N., Poonia, V., Gupta, B. B., & Goyal, M. K. (2021). A novel framework for risk assessment and resilience of critical infrastructure towards climate change. *Technological Forecasting & Social Change, 165*, 120532. https://doi.org/10.1016/j.techfore.2020.120532

Kurz, C. (2020). Comments: Closing the gap: Eliminating the distinction between domestic and international terrorism under federal law. *Temple Law Review, 93*(1), 115–150. https://www.templelawreview.org/lawreview/assets/uploads/2021/01/Kurz_For-Print.pdf

Luskova, M., & Dvorak, Z. (2019). Applying risk management process in critical infrastructure protection. *Interdisciplinary Description of Complex Systems, 17*(1), 7–12. https://doi.org/10.7906/indecs.17.1.2

Meijer, D., Post, J., van der Hoek, J. P., Korving, H., Langeveld, J., & Clemens, F. (2021). Identifying critical elements in drinking water distribution networks using graph theory. *Structure & Infrastructure Engineering: Maintenance, Management, Life-Cycle Design & Performance*, *17*(3), 347–360. https://doi.org/10.1080/15732479.2020.1751664

Molstad, M. (2020). Our inner demons: Prosecuting domestic terrorism. *Boston College Law Review, 61*(1), 339–383. https://lawdigitalcommons.bc.edu/bclr/vol61/iss1/8/

Neudecker, C. H. (2021). *Research in brief: Terrorism risk assessment.* Rutgers Center on Public Security. https://www.rutgerscps.org/uploads/2/7/3/7/27370595/ terrorismriskassessment_brief_neudecker_2021.pdf

Pirbhulal, S., Gkioulos, V., & Katsikas, S. (2021). A systematic literature review on RAMS analysis for critical infrastructures protection*. International Journal of Critical Infrastructure Protection*, *33,* 100427. https://doi.org/10.1016/j.ijcip.2021.100427

Qvortrup, M. (2020). The logic of domestic terrorism revisited: A response to a critic. *Studies in Conflict and Terrorism, 43*(10), 904–909. https://doi.org/10.1080/1057610X.2018.1529376

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing the resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, *25,* 125–138. https://doi.org/10.1016/j.ijcip.2019.03.003

Ren, Z., Guo, J., & Yang, C. (2020). Loss of homeland: a qualitative study of the changes in perception of relocated Sichuan earthquake survivors with posttraumatic stress disorder. *BMC Psychiatry, 20*, 1-11. http://dx.doi.org/10.1186/s12888-020-02789-5

Riedman, D. (2016, May). Questioning the criticality of critical infrastructure: A case study analysis. Homeland Security Affairs, 12, Essay 3. https://www.hsaj.org/articles/10578

Sacco, L. N. (2021, January 15). *Sifting domestic terrorism from hate crime and homegrown violent extremism*. The Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN10299/11

Sedgwick, D., Sedgwick, D., Hawdon, J., & Hawdon, J. (2019). Interagency cooperation in the era of homeland policing: Are agencies answering the call? *American Journal of Criminal Justice, 44*(2), 167–190. https://doi.org/10.1007/s12103-018-9456-4

Sinnar, S. (2019). Separate and unequal: The law of "domestic" and "international" terrorism. *Michigan Law Review, 117*(7), 1333–1404. https://repository.law.umich.edu/mlr/vol117/iss7/2/

Stewart, D. M., & Oliver, W. M. (2021). The adoption of homeland security initiatives in Texas police departments: A contextual perspective. *Criminal Justice Review, 46*(1), 80–98. https://doi.org/10.1177/0734016814551603

Suo, W., Zhang, J., & Sun, X. (2019). Risk assessment of critical infrastructures in a complex interdependent scenario: A four-stage hybrid decision support approach. *Safety Science, 120*, 692–705. https://doi.org/10.1016/j.ssci.2019.07.043

Svegrup, L., Johansson, J., & Hassel, H. (2019). Integration of critical infrastructure and societal consequence models: Impact on Swedish power system mitigation decisions. *Risk Analysis, 39*(9), 1970–1996. https://doi.org/10.1111/risa.13272

Topping, C., Dwyer, A., Michalec, O., Craggs, B., & Rashid, A. (2021). Beware suppliers bearing gifts! Analyzing supply chain cyber security coverage in critical national infrastructure sectorial and cross-sectorial frameworks. *Computers & Security, 108*, 102324. https://doi.org/10.1016/j.cose.2021.102324

Tschantret, J. (2020). Honor and terrorism: Cultural origins of the severity of terrorist attacks. *Social Science Quarterly, 101*(1), 325–345. http://dx.doi.org/10.1111/ssqu.12721

Tulumello, S., & Falanga, R. (2021). Homeland as a multiscalar community: Discontinuities in the U.S. security/safety discourse and practice. *Environment and Planning C: Politics and Space*. https://doi.org/10.1177/23996544211003882

U.S. Department of Homeland Security. (n.d.). *National infrastructure protection plan:* https://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf

Varaine, S. (2019). Revisiting the economics and terrorism nexus: Collective deprivation, ideology, and domestic radicalization in the U.S. (1948–2016). *Journal of Quantitative Criminology, 36*, 667–699. http://dx.doi.org/10.1007/s10940-019-09422-z

Winterfeldt, D., Farrow, R. S., John, R. S., Eyer, J., Rose, A. Z., & Rosoff, H. (2020). Assessing the benefits and costs of homeland security research: A risk-informed methodology with applications for the U.S. Coast Guard. *Risk Analysis, 40*(3), 450–475. https://doi.org/10.1111/risa.13403

Yao, X., Wei, H.-H., Shohet, I. M., & Skibniewski, M. J. (2020). Assessment of terrorism risk to critical infrastructures: The case of a power-supply substation. *Applied Sciences, 10*(20), 7162. http://dx.doi.org/10.3390/app10207162

Abreu, O., Cuesta, A., Balboa, A., & Alvear, D. (2019). On the use of stochastic simulations to explore the impact of human parameters on mass public shooting attacks. *Safety Science, 120*, 941–949. https://doi.org/10.1016/j.ssci.2019.08.038

Anderson, D. A. (2020). Natural gas transmission pipelines: Risks and remedies for host communities. *Energies, 13*(8), 1873. http://dx.doi.org/10.3390/en13081873

Awuzie, B., & Monyane, T. G. (2020). Conceptualizing sustainability governance implementation for infrastructure delivery systems in developing countries: Success factors. *Sustainability, 12*(3), 961. https://doi.org/10.3390/su12030961

Bell, J. (2019). The resistance & the stubborn but unsurprising persistence of hate and extremism in the United States. *Indiana Journal of Global Legal Studies, 26*(1), 305–315. https://doi.org/10.2979/indjglolegstu.26.1.0305

Bell, M. C. (2019). The community in criminal justice: Subordination, consumption, resistance, and transformation. *Du Bois Review, 16*(1), 197–220. http://dx.doi.org/10.1017/S1742058X1900016X

Bencie, L., & Araboghli, S. (2019). Let’s be blunt: Time for a new critical infrastructure sector? *Journal of Counterterrorism & Homeland Security International, 25*(1), 40–41. https://search-ebscohost-com.ezproxy.liberty.edu/login.aspx?direct=true&db=poh&AN=138564451&site=ehost-live&scope=site

Berryman, C. (2020). Holding social media providers liable for acts of domestic terrorism. *Florida Law Review, 72*(6), 1329. http://www.floridalawreview.com/2021/holding-social-media-providers-liable-for-acts-of-domestic-terrorism/

Bickham, R. A. (2021). Using remote monitoring, evaluate pipeline lightning immunity. *Pipeline & Gas Journal, 248*(3), 32–33. https://www-proquest-com.ezproxy.liberty.edu/docview/2509368141?pq-origsite=summon

Boukalas, C. (2019). The *Prevent* paradox: Destroying liberalism in order to protect it. *Crime, Law and Social Change, 72*(4), 467–482. https://doi.org/10.1007/s10611-019-09827-8

Brenna, A., Beretta, S., & Ormellese, M. (2020). AC corrosion of carbon steel under cathodic protection condition: Assessment, criteria, and mechanism. A review. *Materials, 13*(9), 2158. https://doi.org/10.3390/ma13092158

Brod, T. J. (2018). *Police managers' transformational leadership impact on change initiatives in police organizations* (Order No. 13423043) [Doctoral dissertation, Capella University]. ProQuest Dissertations & Theses Global.

Brogan, M., Rusciano, F. L., Thompson, V., & Walden, K. (2020, January). Perceptions of terrorism and counterterrorism: Fear, risk, and the 2016 Trump effect. *Journal of Homeland Security & Emergency Management, 17*(1), 1–9. 10.1515/jhsem-2018-0023

Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems & Decisions, 41*, 341–376. https://doi.org/10.1007/s10669-020-09795-8

Carmack, B. (2020). My brother's keeper: Using the foreign intelligence toolbox on domestic terrorism. *Mitchell Hamline Law Review, 46*(5), Article 4. https://open.mitchellhamline.edu/mhlr/vol46/iss5/4/

Chalk, P. (2020). Research notes: Domestic counter-terrorist intelligence structures in the United Kingdom, France, Canada, and Australia. *Studies in Conflict and Terrorism*. https://doi.org/10.1080/1057610X.2019.1680186

Chatterjee, S., Brigantic, R. T., & Waterworth, A. M. (Eds.). (2021). *Applied risk analysis for guiding homeland security policy and decisions.* John Wiley & Sons. https://www.wiley.com/en-us/Applied+Risk+Analysis+for+Guiding+Homeland+Security+Policy+and+Decisions+-p-9781119287469

Christian, M. (2020). US House infrastructure plan includes $34.3B in clean energy investments. *SNL Energy Power Daily*. https://www-ProQuest-com.ezproxy.liberty.edu/docview/2349707297?pq-origsite=summon

Comiskey, J. (2018). Theory for homeland security. Journal of Homeland Security Education, 7, 29–45. https://jsire.org/theory-for-homeland-security

Derks, J., Giessen, L., & Winkel, G. (2020). COVID-19-induced visitor boom reveals the importance of forests as critical infrastructure. *Forest Policy and Economics, 118*, 102253–102253. https://doi.org/10.1016/j.forpol.2020.102253

DiChristopher, T. (2020). *Cyberattack uncovers shortfalls in natural gas pipeline security.* SNL Financial LC. https://www-proquest-com.ezproxy.liberty.edu/docview/2363598104?pq-origsite=summon

Durrett, R. (2019). *Probability: Theory and examples* (5th ed.). Cambridge University Press. https://doi.org/10.1017/9781108591034

Ekström, T., Sundling, R., Burke, S., & Harderup, L. (2021). Probabilistic risk analysis and building performance simulations—building design optimization and quantifying stakeholder consequences. *Energy and Buildings, 252*, 111434. https://doi.org/10.1016/j.enbuild.2021.111434

Eyberg, I. (2019). To reduce security vulnerabilities in downstream facilities, try uni-kernels. *Hydrocarbon Processing*. https://www.hydrocarbonprocessing.com/magazine/2019/july-2019/special-focus-the-digital-refinery/to-reduce-security-vulnerabilities-in-downstream-facilities-try-unikernels

Fiebig, J. N., & Christopher, J. (2018). Female leadership styles: Insights from Catholic women religious on leading through compassion. *Pastoral Psychology, 67*(5), 505–513. https://doi.org/10.1007/S11089-018-0829-X

Filusch, T. (2021). Risk assessment for financial accounting: Modeling probability of default. *The Journal of Risk Finance, 22*(1), 1–15. https://doi.org/10.1108/JRF-02-2020-0033

Forman, P. J. (2020). Security and the subsurface: Natural gas and the visualization of possibility spaces. *Geopolitics, 25*(1), 143–166. https://doi.org/10.1080/14650045.2018.1513918

Gaibulloev, K., & Sandler, T. (2019). Terrorism and affinity of nations. *Public Choice, 178*(3-4), 329–347. http://dx.doi.org/10.1007/s11127-018-0611-8

Ganesh, B., & Bright, J. (2020). Countering extremists on social media: Challenges for strategic communication and content moderation. *P&I: Policy & Internet, 12*(1). 6–19. https://doi.org/10.1002/poi3.236

Godwin, R. E. (2019). *Navigating change: How emotional intelligence competencies drive successful transformational change within the electric utility industry* (Order No. 13900886) [Doctoral dissertation, Chicago School of Professional Psychology]. Available from ProQuest Dissertations & Theses Global.

Good, A. (2020). *Cyberattacks can weaken pipeline companies' credit, Moody says after the incident.* SNL Financial LC. https://www-proquest-com.ezproxy.liberty.edu/docview/2370248191?pq-origsite=summon

Goswami, A., O'Brien, K. E., Dawson, K. M., & Hardiman, M. E. (2018). Mechanisms of corporate social responsibility: The moderating role of transformational leadership. *Ethics & Behavior, 28*(8), 644–661. https://doi.org/10.1080/10508422.2018.1467764

Grimmett, G. R. (2021). Harry Kesten's work in probability theory. *Probability Theory and Related Fields, 181*(1-3), 17–55. https://doi.org/10.1007/s00440-021-01046-4

Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behavior: An examination of the full-range leadership theory. *Information Systems Journal, 29*(2), 340–362. https://doi.org/10.1111/isj.12202

Hayes, J., Sandri, O., & Holdsworth, S. (2021). "More likely to be killed by a coconut": Varying professional perceptions of risk impacting residential development planning around pipelines. *Journal of Risk Research, 24*(2), 183–197. https://doi.org/10.1080/13669877.2019.1694963

Herring, S. R., IV. (2020). *Contributing to organizational theory: Studying the business operations management of the homeland security enterprise.* ProQuest Dissertations Publishing. https://search-proquest-com.ezproxy.liberty.edu/docview/2388038183?pq-origsite=summon

Holzmann, T., & Smith, J. C. (2021). The shortest path interdiction problem with randomized interdiction strategies: Complexity and algorithms. *Operations Research, 69*(1), 82–99. https://doi.org/10.1287/opre.2020.2023

Hunter, L. Y., Griffith, C. E., & Warren, T. (2020). Internet connectivity and domestic terrorism in democracies. *International Journal of Sociology, 50*(3), 201–219. https://doi.org/10.1080/00207659.2020.1757297

Hurdle-Lightfoot, C. L. (2020). *Risk assessment strategies to reduce profitability losses from pipeline accidents in the natural gas industry* (Order No. 27742437) [Doctoral dissertation, Walden University]. ProQuest Dissertations and Theses Global.

Hyung-Woo, L. (2018). Linking leadership practices to performance of the U.S. federal agencies. *International Journal of Manpower, 39*(3), 434–454. http://dx.doi.org/10.1108/IJM-09-2016-0168

INGAA, API laud congressional passage of PIPES Act. (2020, December 22). *Pipeline & Gas Journal, 248*(1). https://pgjonline.com/news/2020/12-december/ingaa-api-laud-congressional-passage-of-pipes-act

Jaimes, M. A., García-Soto, A. D., Martín del Campo, J. Osvaldo, & Pozos-Estrada, A. (2020). Probabilistic risk assessment on wind turbine towers subjected to cyclone-induced wind loads. *Wind Energy (Chichester, England), 23*(3), 528–546. https://doi.org/10.1002/we.2436

Jasko, K., & LaFree, G. (2020). Who is more violent in extremist groups? A comparison of leaders and followers. *Aggressive Behavior, 46*(2), 141–150. https://doi.org/10.1002/ab.21865

Jiang, L., & Liao, H. (2021). Double-quantified linguistic variable. *Information Sciences, 545,* 207–222. https://doi.org/10.1016/j.ins.2020.08.026

Johnson, C. A., Flage, R., & Guikema, S. D. (2021). Feasibility study of PRA for critical infrastructure risk analysis. *Reliability Engineering & System Safety, 212,* 107643. https://www.sciencedirect.com/science/article/pii/S0951832021001848

Josephine, A., Fischabcher-Smith, D., & Fischabcher-Smith, M. (2020). Inherent complexities of a multi-stakeholder approach to building community resilience. *International Journal of Disaster Risk Science, 11*(1), 32–45. http://dx.doi.org/10.1007/s13753-020-00246-1

Karbowski, A., Malinowski, K., Szwaczyk, S., & Jaskóła, P. (2019). Critical infrastructure risk assessment using Markov chain model. *Journal of Telecommunications and Information Technology, (2),* 15–20. http://dx.doi.org/10.26636/jtit.2019.130819

Kessler, V. (2020). The beauty of spiritual leadership: A theological-aesthetical approach to leadership. *Hervormde Teologiese Studies, 76*(2). http://dx.doi.org/10.4102/hts.v76i2.5898

King James Bible. (2021). King James Bible Online. https://www.kingjamesbibleonline.org/ (Original work published 1769)

Knight, E., & Gekker, A. (2020). Mapping interfacial regimes of control: Palantir’s ICM in America’s post-9/11 security technology infrastructures. *Surveillance & Society, 18*(2), 231–243. https://doi.org/10.24908/ss.v18i2.13268

Krueger, B. S., Best, S. J., & Johnson, K. (2020). Assessing dimensions of the security-liberty trade-off in the United States. *Surveillance & Society, 18*(1), 104–120. https://doi.org/10.24908/ss.v18i1.10419

Kruse, P. M., Schmitt, H. C., & Greiving, S. (2021). Systemic criticality—a new assessment concept improving the evidence basis for CI protection. *Climatic Change, 165*(1-2), 2-2. https://doi.org/10.1007/s10584-021-03019-x

Kuczyński, S., Łaciak, M., Olijnyk, A., Szurlej, A., & Włodek, T. (2019). Techno-economic assessment of turboexpander application at natural gas regulation stations. *Energies, 12*(4). http://dx.doi.org/10.3390/en12040755

LaFree, G., Jiang, B., & Porter, L. C. (2020). Prison and violent political extremism in the United States. *Journal of Quantitative Criminology, 36*(3), 473–498. https://doi.org/10.1007/s10940-019-09412-1

Laguardia, F. (2020). Considering a domestic terrorism statute and its alternatives. *Northwestern University Law Review, 114*(4), 1061–1099. https://scholarlycommons.law.northwestern.edu/nulr/vol114/iss4/4/

Lemos-Cano, S., & McCalley, J. (2019). Co-optimized analysis and design of electric and natural gas infrastructures. *Energies, 12*(10). http://dx.doi.org/10.3390/en12102012

Loveless, R., Jr. (2019). *An organization in transition: An ethnographic case study of structural and cultural change* (Order No. 13897213) [Doctoral dissertation, Wilmington University]. ProQuest Dissertations & Theses Global.

Luskova, M., & Dvorak, Z. (2019). Applying risk management process in critical infrastructure protection. *Interdisciplinary Description of Complex Systems, 17*(1), 7–12. http://dx.doi.org/10.7906/indecs.17.1.2

Maertens, A., Golden, E., Luechtefeld, T. H., Hoffmann, S., Tsaioun, K., & Hartung, T. (2022). Probabilistic risk assessment: The keystone for the future of toxicology. ALTEX, *Alternatives to Animal Experimentation, 39*(1), 3–29. https://doi.org/10.14573/altex.2201081

Mahoney, C. W. (2020). Empty threats: How extremist organizations bluff in terrorist campaigns. *Studies in Conflict and Terrorism, 43*(12), 1043–1063. https://doi.org/10.1080/1057610X.2018.1514093

McAleenan, K. K., & Plofchan, Thomas K., III. (2020). Domestic terror is a rising threat. *The Washington Post, Monday, 12, October 2020.* http://ezproxy.liberty.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fnewspapers%2Fdomestic-terror-is-rising-threat%2Fdocview%2F2449771685%2Fse-2%3Faccountid%3D12085

McCreight, R. (2019). Grid collapse security, stability and vulnerability issues: Impactful issues affecting nuclear power plants, chemical plants and natural gas supply systems. *Journal of Homeland Security & Emergency Management, 16*(1). https://doi.org/10.1515/jhsem-2018-0021

McIlhatton, D., Berry, J., Chapman, D., Christensen, P. H., Cuddihy, J., Monaghan, R., & Range, D. (2020). Protecting crowded places from terrorism: An analysis of the current considerations and barriers inhibiting the adoption of counterterrorism protective security measures. *Studies in Conflict and Terrorism, 43*(9), 753–774. https://doi.org/10.1080/1057610X.2018.1507311

Milton, D., & Price, B. (2020). Too central to fail? Terror networks and leadership decapitation. *International Interactions, 46*(3), 309–333. https://doi.org/10.1080/03050629.2020.1719406

Montag, C., Elhai, J. D., & Dagum, P. (2021). Show me your smartphone, and then I will show you your brain structure and brain function. *Human Behavior and Emerging Technologies, 3*(5), 891–897. https://doi.org/10.1002/hbe2.272

Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and Justice*, 42(1), 199–263. https://doi.org/10.1086/670398

Newbill, C. M. (2019). Defining critical infrastructure for a global application. *Indiana Journal of Global Legal Studies, 26*(2), 761–780. https://doi.org/10.2979/indjglolegstu.26.2.0761

Nguyen, N. (2019). “The eyes and ears on our frontlines”: Policing without police to counter violent extremism. *Surveillance & Society, 17*(3/4), 322–337. https://doi.org/10.24908/ss.v17i3/4.8142

Obadi, S. M., & Korček, M. (2019). Current drivers and price development on natural gas markets—focus on Europe. *Surveying Geology & Mining Ecology Management* (SGEM). http://dx.doi.org/10.5593/sgem2019/1.2/S06.096

Piazza, J. A. (2020). Politicians hate speech and domestic terrorism. *International Interactions, 46*(3), 431–453. https://doi.org/10.1080/03050629.2020.1739033.

Quinn, C. (2020). *Alarm forecasting in natural gas pipelines* [Master's thesis, Marquette University].e-Publications@Marquette. https://epublications.marquette.edu/theses_open/577/

Quitzow, R., Bersalli, G., Eicke, L., Jahn, J., Lilliestam, J., Lira, F., Marian, A., Süsser, D., Thapar, S., Weko, S., Williams, S., & Xue, B. (2021). The COVID-19 crisis deepens the gulf between leaders and laggards in the global energy transition. *Energy Research & Social Science, 74,* 101981. https://doi.org/10.1016/j.erss.2021.101981

Rich, P. B. (2020). Hollywood and cinematic representations of far-right domestic terrorism in the U.S. *Studies in Conflict and Terrorism, 43*(2), 161–182. https://doi.org/10.1080/1057610X.2018.1446295

Richardson, A. D. (2020). *Examining leadership and emotional intelligence of police leaders in rural policing agencies* (Order No. 28002034) [Doctoral dissertation, Capella University]. ProQuest Dissertations & Theses Global.

Saada, M. (2021). *A probabilistic framework using dynamic Bayesian networks for human activity recognition and tracking* [Doctoral dissertation, Loughborough University]. https://repository.lboro.ac.uk/articles/thesis/A_probabilistic_framework_using_dynamic_Bayesian_networks_for_human_activity_recognition_and_tracking/16895362

Saito, N. T. (2019). "Identity extremism." *National Lawyers Guild Review, 75*(3), 1–16. https://www.nlg.org/nlg-review/article/identity-extremism/

Sarteschi, C. M. (2020). *Sovereign citizens: A psychological and criminological analysis*. Springer. https://link-springer com.ezproxy.liberty.edu/book/10.1007%2F978-3-030-45851-5

Sauter, K. (2020). Pipe dreams: Streamlining cybersecurity regulatory authority over the energy industry to increase national security. *Administrative Law Review, 72*(3), 507–532. http://www.administrativelawreview.org/wp-content/uploads/2020/09/12.-ALR-72.3_Sauter-Comment_FINAL.pdf

Schlette, D., Böhm, F., Caselli, M., & Pernul, G. (2021). Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security, 20*(1), 21–38. https://doi.org/10.1007/s10207-020-00490-y

Schuurman, B., Lindekilde, L., Malthaner, S., O'Connor, F., Gill, P., & Bouhana, N. (2019). End of the lone wolf: The typology that should not have been. *Studies in Conflict & Terrorism, 42*(8), 771–778. https://doi.org/10.1080/1057610X.2017.1419554

Sheth, S. (2019). FBI Agents Association urges Congress to make domestic terrorism a federal crime in the wake of Dayton and El Paso mass shootings. *Business Insider.* http://ezproxy.liberty.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fnewspapers%2Ffbi-agents-association-urges-congress-make%2Fdocview%2F2399297583%2Fse-2%3Faccountid%3D12085.

Simonelli, I. S. (2020). Alaska's giving pipeline: Philanthropy in the oil and gas industry. *Alaska Business Monthly, 37*(5). https://digital.akbizmag.com/issue/may-2020/alaskas-giving-pipeline/

Standley, V. H., Nuño, F. G., & Sharpe, J. W. (2020). Fusing attack detection and severity probabilities: a method for computing minimum-risk war decisions. *Computing, 102*(6), 1385–1408. http://dx.doi.org/10.1007/s00607-020-00801-0

Steckler, E. L., & Waddock, S. (2018). Self-sustaining practices of successful social change agents: A retreats framework for supporting transformational change. *Humanistic Management Journal, 2*(2), 171–198. http://dx.doi.org/10.1007/s41463-017-0031-9

Strang, K. D. (2018). Strategic analysis of CSFs for not-for-profit organizations. *Measuring Business Excellence, 22*(1), 42–63. https://doi.org/10.1108/MBE-07-2016-0035

Suo, W., Wang, L., & Li, J. (2021). Probabilistic risk assessment for interdependent critical infrastructures: A scenario-driven dynamic stochastic model. *Reliability Engineering & System Safety, 214*, 107730. https://doi.org/10.1016/j.ress.2021.107730

Tamborini, R., Hahn, L., Aley, M., Prabhu, S., Baldwin, J., Sethi, N., Novotny, E., Klebig, B., & Hofer, M. (2020). The impact of terrorist attack news on moral intuitions. *Communication Studies, 71*(4), 511–527. https://doi.org/10.1080/10510974.2020.1735467

Taquechel, E. F., & Saitgalina, M. (2018). Risk-based performance metrics for critical infrastructure protection? A framework for research and analysis. *Homeland Security Affairs, 14*, Article 8. https://www.hsaj.org/articles/14699

Tata, P., & DeCotis, P. A. (2019). Natural gas infrastructure development—risks and responsibilities. *Natural Gas & Electricity, 36*(1), 1–10. https://doi.org/10.1002/gas.22130

Tezak, C. (2019). A policy analyst's view on litigation risk facing natural gas pipelines. *Energy Law Journal, 40*(2), 209–241. https://www.eba-net.org/assets/1/6/7.[Tezak][Final][209-241].pdf

Tung, Y. (2019). An information operations theory of domestic counterterrorism efforts. *South Carolina Law Review, 71*(2), 523–602. https://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=146419238&S=R&D=asn&EbscoContent=dGJyMNHX8kSeprQ4y9fwOLCmsEmeqK9Ssqy4TLOWxWXS&ContentCustomer=dGJyMOrf4H3w6vdT69fnhrnb5ofx6gAA

U.S. Department of Homeland Security (2021a). *DHS announces new cybersecurity requirements for critical pipeline owners and operators.* https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

U.S. Department of Homeland Security (2021c). *National Terrorism Advisory System*. https://www.dhs.gov/sites/default/files/ntas/alerts/21_0127_ntas-bulletin.pdf

U.S. Department of Homeland Security. (2021b). *National Infrastructure Protection Plan*. https://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf

Uberti, D., & Stupp, C. (2021). Colonial pipeline hack sparks questions about oversight; pipelines lack security regulations like those imposed on utilities and the maritime sector. *WSJ Pro. Cyber Security*. https://www-proquest-com.ezproxy.liberty.edu/docview/2524524030?pq-origsite=summon

Wang, H., Jin, Y., & Tan, X. (2020). Study on sustainable development of the transnational power grid interconnection projects under diversified risks based on variable weight theory and Bayesian network. *Mathematical Problems in Engineering, 2020,* 1–10. https://doi.org/10.1155/2020/5361561

Weeks, D. (2019). Barking Mosque and Quintessential Insight: Overcoming the problematic government/community counterterrorism partnership in the U.K. *Studies in Conflict & Terrorism, 42*(8), 735–754. https://doi.org/10.1080/1057610X.2018.1425087

Wei, L., Du, H., Mahesar, Q., Al Ammari, K., Magee, D. R., Clarke, B., Dimitrova, V., Gunn, D., Entwisle, D., Reeves, H., & Cohn, A. G. (2020). A decision support system for urban infrastructure inter-asset management employing domain ontologies and qualitative uncertainty-based reasoning. *Expert Systems with Applications*, *158*, 113461. https://doi.org/10.1016/j.eswa.2020.113461

Wibeck, V., Björn-Ola Linnér, Alves, M., Asplund, T., Bohman, A., Boykoff, M. T., Feetham, P. M., Huang, Y., Nascimento, J., Rich, J., Rocha, C. Y., Vaccarino, F., & Shi, X. (2019). Stories of transformation: A cross-country focus group study on sustainable development and societal change. *Sustainability, 11*(8). http://dx.doi.org/10.3390/su11082427

Wilcox, P. (2020). An argument for establishing a National Security Council interagency information warfare directorate Part III. *Journal of Information Warfare, 19*(2), 108–115. https://www.jstor.org/stable/27033624

Xiong, J., Isgandarova, N., & Panton, A. E. (2020). COVID-19 demands theological reflection: Buddhist, Muslim, and Christian perspectives on the present pandemic. *International Journal of Practical Theology*, *24*(1), 5–28. https://doi.org/10.1515/ijpt-2020-0039

Zulli, D., Coe, K., Isaacs, Z., & Summers, I. (2021). Media coverage of the unfolding crisis of domestic terrorism in the United States, 1990–2020. *Public Relations Inquiry, 20,* 46147. https://doi.org/10.1177/2046147X21996015

Bowater, R. J., & Guzmán-Pantoja, L. E. (2019). Bayesian, classical and hybrid methods of inference when one parameter value is special. *Journal of Applied Statistics, 46*(8), 1417–1437. https://doi.org/10.1080/02664763.2018.1548585

Chatterjee, S., Brigantic, R. T., & Waterworth, A. M. (2021). *Applied risk analysis for guiding homeland security policy and decisions.* John Wiley & Sons.

Chalgham, W. (2020). *System-level prognosis and health monitoring modeling framework and software implementation for gas pipeline system integrity management* (Publication No. 28256079) [Doctoral dissertation, University of California, Los Angeles]. ProQuest Dissertations & Theses Global.

Comiskey, J. (2018). Theory for homeland security. *Journal of Homeland Security Education, 7,* 29–45. https://jsire.org/theory-for-homeland-security

Hayes, A. (2022). *Bayes' theorem definition.* Investopedia. https://www.investopedia.com/terms/b/bayes-theorem.asp

Kammouh, O., Gardoni, P., & Cimellaro, G. P. (2020). Probabilistic framework to evaluate the resilience of engineering systems using Bayesian and dynamic Bayesian networks. *Reliability Engineering & System Safety, 198,* Art. 106813. https://doi.org/10.1016/j.ress.2020.106813

Kong, J., & Simonovic, S. P. (2019). Probabilistic multiple hazard resilience model of an interdependent infrastructure system. *Risk Analysis, 39*(8), 1843–1863. https://doi.org/10.1111/risa.13305

Kubo, K., Jang, S., Takashi, T., & Yamaguchi, A. (2021). Quasi-Monte Carlo sampling method for simulation-based dynamic probabilistic risk assessment of nuclear power plants.

Journal of Nuclear Science and Technology, *59*(3), 357–367. https://doi.org/10.1080/00223131.2021.1971119

Kumar, S., Saket, R. K., Dheer, D. K., Holm-Nielsen, J., & Sanjeevikumar, P. (2020). Reliability enhancement of electrical power system including impacts of renewable energy sources: A comprehensive review. *IET Generation, Transmission & Distribution, 14*(10), 1799–1815. https://doi.org/10.1049/iet-gtd.2019.1402

Nouri Qarahasanlou, A., Zamani, A., Barabadi, A., & Mokhberdoran, M. (2021). Resilience assessment: A performance-based importance measure. *Energies (Basel), 14*(22), 7575. https://doi.org/10.3390/en14227575

Oates, C. J., & Sullivan, T. J. (2019). A modern retrospective on probabilistic numerics. *Statistics and Computing, 29*(6), 1335–1351. https://doi.org/10.1007/s11222-019-09902-z

Ongkowijoyo, C., & Doloi, H. (2017). Determining critical infrastructure risks using social network analysis. *International Journal of Disaster Resilience in the Built Environment, 8*(1), 5–26. http://dx.doi.org.ezproxy.liberty.edu/10.1108/IJDRBE-05-2016-0016

Suo, W., Wang, L., & Li, J. (2021). Probabilistic risk assessment for interdependent critical infrastructures: A scenario-driven dynamic stochastic model. *Reliability Engineering & System Safety, 214,* Art. 107730. https://doi.org/10.1016/j.ress.2021.107730

Thöns, S., & Stewart, M. G. (2020). On the cost-efficiency, significance, and effectiveness of terrorism risk reduction strategies for buildings. *Structural Safety, 85,* Art. 101957. https://doi.org/10.1016/j.strusafe.2020.101957

Tendeiro, J. N., & Kiers, H. A. L. (2019). A review of issues about null hypothesis Bayesian testing. *Psychological Methods, 24*(6), 774–795. https://doi.org/10.1037/met0000221

Zhou, T., Modarres, M., & Droguett, E. L. (2021). Multiunit nuclear power plant probabilistic risk assessment: A comprehensive survey. *Reliability Engineering & System Safety, 213*, Art. 107782. https://doi.org/10.1016/j.ress.2021.107782

Che-Castaldo, J., Cousin, R., Stefani, D., Deng, G., Feng, M.-L. E., Gupta, R. K., Hong, D., McGranaghan, R. M., Owolabi, O. O., Qu, T., Ren, W., Schafer, T., L. J., Sharma, A., Shen, C., Sherman, M. G., Sunter, D. A., Tao, B., Wang, L., & Matteson, D. S. (2021). Critical risk indicators (CRIs) for the electric power grid: A survey and discussion of interconnected effects. *Environment Systems & Decisions, 41*(4), 594–615. https://doi.org/10.1007/s10669-021-09822-2

Huse, J. (2018). Crowdsourcing threat analysis; applying a “Superforecasting” methodology to detection of homegrown violence. *Homeland Security Affairs.* Naval Postgraduate School Monterey, California. Thesis Approved for public release unlimited. https://www-proquest-com.ezproxy.liberty.edu/docview/2206256062?pq-origsite=summon

Karki, I. (2020). *Analyzing critical pipeline crossings at highways* (Order No. 27962861) [Doctoral dissertation, California State University]. ProQuest Central.

King James Bible. (2021). King James Bible Online. https://www.kingjamesbibleonline.org/ (Original work published 1769)

Langat, P. K., Kumar, L., & Koech, R. (2019). Identification of the most suitable probability distribution models for maximum, minimum, and mean streamflow. *Water, 11*(4), 734. https://doi.org/10.3390/w11040734

Nouri Qarahasanlou, A., Zamani, A., Barabadi, A., & Mokhberdoran, M. (2021). Resilience assessment: A performance-based importance measure. *Energies (Basel), 14*(22), 7575. https://doi.org/10.3390/en14227575

Tan, S., Weinert, D., Joseph, P., & Moinuddin, K. (2020). Impact of technical, human, and organizational risks on reliability of fire safety systems in high-rise residential buildings: Applications of an integrated probabilistic risk assessment model. *Applied Sciences, 10*(24), 8918. http://dx.doi.org/10.3390/app10248918

Valentin Torres, A. H. (2020). Applicability of predictive modeling on a network enterprise risk management critical infrastructure (Order No. 28391145) [Doctoral dissertation, Marymount University]. ProQuest Central.

Aven, T. (2008). *Risk analysis: Assessing uncertainties beyond expected values and probabilities* (1st ed.). Wiley. https://doi.org/10.1002/9780470694435

Chatterjee, S., Brigantic, R. T., & Waterworth, A. M. (2021). *Applied risk analysis for guiding homeland security policy and decisions.* John Wiley & Sons. https://doi.org/10.1002/9781119287490

Cheng, Y., Elsayed, E. A., & Huang, Z. (2022). Systems resilience assessments: A review, framework, and metrics. *International Journal of Production Research, 60*(2), 595–622. https://doi.org/10.1080/00207543.2021.1971789

Enhancing the Organization of the United States Department of Homeland Security to Account for National Risk. (2020). *Homeland Security Affairs, XVI.* http://ezproxy.liberty.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fenhancing-organization-united-states-department%2Fdocview%2F2522295241%2Fse-2%3Faccountid%3D12085

Fjaeran, L., & Aven, T. (2021). Making visible the less visible—how the use of an uncertainty-based risk perspective affects risk attenuation and risk amplification. *Journal of Risk Research, 24*(6), 673–691. https://doi.org/10.1080/13669877.2019.1687579

Flage, R., Aven, T., & Berner, C. L. (2018). A comparison between a probability bounds analysis and a subjective probability approach to express epistemic uncertainties in a risk assessment context—a simple illustrative example. *Reliability Engineering & System Safety, 169*, 1–10. https://doi.org/10.1016/j.ress.2017.07.016

Glette-Iversen, I., Aven, T., & Flage, R. (2022). The concept of plausibility in a risk analysis context: Review and clarifications of defining ideas and interpretations. *Safety Science, 147*, 105635. https://doi.org/10.1016/j.ssci.2021.105635

King James Bible. (2021). King James Bible Online. https://www.kingjamesbibleonline.org/ (Original work published 1769)

Logan, T. M., Aven, T., Guikema, S., & Flage, R. (2021). The role of time in risk and risk analysis: Implications for resilience, sustainability, and management. *Risk Analysis, 41*(11), 1959–1970. https://doi.org/10.1111/risa.13733

Oliva, G., Faramondi, L., Setola, R., Tesei, M., & Zio, E. (2021). A multi-criteria model for the security assessment of large-infrastructure construction sites. *International Journal of Critical Infrastructure Protection, 35,* 100460. https://doi.org/10.1016/j.ijcip.2021.100460

Ongkowijoyo, C., & Doloi, H. (2017). Determining critical infrastructure risks using social network analysis. *International Journal of Disaster Resilience in the Built Environment, 8*(1), 5–26. http://dx.doi.org.ezproxy.liberty.edu/10.1108/IJDRBE-05-2016-0016

Picoco, C., Rychkov, V., & Aldemir, T. (2020). A framework for verifying dynamic probabilistic risk assessment models. *Reliability Engineering & System Safety, 203*, 107099. https://doi.org/10.1016/j.ress.2020.107099

Silva, L. M. F., de Oliveira, Ana Camila Rodrigues, Leite, M. S. A., & Marins, F. A. S. (2021). Risk assessment model using conditional probability and simulation: Case study in a piped gas supply chain in Brazil. *International Journal of Production Research, 59*(10), 2960–2976. https://doi.org/10.1080/00207543.2020.1744764

Suave, G., & Van Acker, K. (2021). Integrating life cycle assessment (LCA) and quantitative risk assessment (QRA) to address model uncertainties: Defining a landfill reference case under varying environmental and engineering conditions. *International Journal of Life Cycle Assessment*, *26*(3), 591–603. http://dx.doi.org/10.1007/s11367-020-01848-z

Suo, W., Wang, L., & Li, J. (2021). Probabilistic risk assessment for interdependent critical infrastructures: A scenario-driven dynamic stochastic model. *Reliability Engineering & System Safety, 214*, Art. 107730. https://doi.org/10.1016/j.ress.2021.107730

Winterfeldt, D., Farrow, R. S., John, R. S., Eyer, J., Rose, A. Z., & Rosoff, H. (2020). Assessing the benefits and costs of homeland security research: A risk-informed methodology with applications for the U.S. Coast Guard. *Risk Analysis, 40*(3), 450–475. https://doi.org/10.1111/risa.13403

Zio, E., Mustafayeva, M., & Montanaro, A. (2022). A Bayesian belief network model for the risk assessment and management of premature screen-out during hydraulic fracturing. *Reliability Engineering & System Safety, 218*, 108094. https://doi.org/10.1016/j.ress.2021.108094