Protecting Critical Infrastructure for Disasters: NLP-Based Automated Information Retrieval to Generate Hypothetical Cyberattack Scenarios

Christin Salley[1]; Neda Mohammadi, Ph.D., A.M.ASCE[2]; and John E. Taylor, Ph.D., M.ASCE[3]

Abstract: Cyberattacks disrupt systems, leaving critical infrastructure vulnerable to adversaries, especially during natural disasters. Furthermore, when both a cyberattack and a natural disaster occur concurrently, there are limited tools to ensure further damage beyond the physical is not experienced in crucial societal systems, such as emergency services, which need to operate during any type of hazard. Two prominent knowledge bases for adversary attacks in the cybersecurity community are the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Enterprise Matrix and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Existing processes to derive possible attack methodologies in general from such sources are largely manual and time-consuming. It is essential to automate the information retrieval process to improve efficiency and free up resources for identifying potential cyberattacks. It is also important to identify preventive measures with both human-made and natural hazards in mind. We propose an approach that incorporates Natural Language Processing (NLP) to automatically generate sets of attack paths from the technique descriptions in the Matrix, with both cyber-based and emergency management–based contexts, then map these techniques to the Framework to identify potential relationships between techniques and outlined protective actions. The approach generates outputs showing potential pathways an adversary can take to infiltrate a system, and its respective defense action based on similarity measures. The similarities between techniques and the Framework are evaluated with p-values to determine relevancy of pairings. The results of this study provide an approach to more quickly and effectively assess potential cyberattacks toward protecting critical infrastructure that can be utilized in broader vulnerability analyses, considering contextual data to represent both cyber and natural disaster events. **DOI: 10.1061/JITSE4.ISENG-2407.**

Introduction

Community resilience has been a national priority, with a key component being the safeguarding of critical infrastructure. The risk of natural disasters on critical infrastructure has been studied extensively; however, when the tragic events of the September 11 attacks occurred in 2001, the United States was shown the crucial need to anticipate both human-made and natural attacks on infrastructure (Grigg 2003). This created a shift in legislation for improving security measures and the creation of new federal departments and initiatives to combat both cyber and physical threats to infrastructure. The repercussions of disruptions to critical infrastructure can have severe consequences for society including loss of life, economic disruption, and social instability. Simultaneous consideration of security and disaster preparedness has been identified as crucial in addressing these challenges (Grigg 2003).

Critical infrastructure and cybersecurity research has identified ways to bridge gaps between emergency management and the cybersecurity space. These include communicating about cyber crises (Bolton 2013), building information science-based data systems to equip communities to better manage natural disasters (Li et al. 2014), and expressing concern for a lack of cyber situational awareness during natural disasters (Walker et al. 2010) more effectively. Effective emergency management systems reduce the impacts of disasters and ensure that critical infrastructure can continue to function during and after an emergency event. Many organizations rely on telecommunications and computational systems to support their emergency response efforts as data collection and real-time information exchange occurs within disaster management (Seba et al. 2019). Preparing for cybercrimes and intrusions of these systems aids organizations' defense against potential disruptions and should be integrated into emergency response plans (Janczewski and Colarik 2007). It is critical to keep these disaster management systems safe not only for communication and information exchange between and within organizations, but also to keep the private, identifiable details of citizens uncompromised (Sutedi et al. 2021). If an adversary successfully attacks such systems, the intruder can get information such as name, date of birth, address, insurance provider, etc., and the damage can range from fraud to psychosocial harm (Argaw et al. 2020).

As cyberattacks are seen steadily increasing in critical infrastructure sectors (Ponemon 2016), interdependencies within critical infrastructure systems continue to emerge as a focal point in the endeavor to protect them. Notably, an attack on one sector can trigger disruptions or failures across multiple sectors, as highlighted by the Cybersecurity and Infrastructure Security Agency's (CISA) identification of interconnected critical infrastructure

[1]Ph.D. Candidate, School of Civil and Environmental Engineering, Georgia Institute of Technology, Atlanta, GA 30332. Email: csalley3@gatech.edu

[2]City Infrastructure Analytics Director, School of Civil and Environmental Engineering, Georgia Institute of Technology, Atlanta, GA 30332. Email: nedam@gatech.edu

[3]Frederick Law Olmsted Professor, School of Civil and Environmental Engineering, Georgia Institute of Technology, Atlanta, GA 30332 (corresponding author). ORCID: https://orcid.org/0000-0002-8949-3248. Email: jet@gatech.edu

Note. This manuscript was submitted on August 8, 2023; approved on February 7, 2024; published online on May 24, 2024. Discussion period open until October 24, 2024; separate discussions must be submitted for individual papers. This paper is part of the ***Journal of Infrastructure Systems***, © ASCE, ISSN 1076-0342.

sectors (CISA 2023). Consider how emergency management efforts tied to critical infrastructure (i.e., the emergency services sector) are dependent on the Communications Sector, Healthcare and Public Health Sector, and the Nuclear Reactors, Materials, and Waste Sector; these noted sectors further connect emergency services to other sectors that could be affected if it is harmed such as the Energy Sector, Information Technology Sector, Transportation Sector, and more (CISA 2023). Emergency services are a prime example of a system of systems within critical infrastructure that, if made vulnerable to both a natural disaster and a cyber threat, could lead to detrimental impacts. If a cyberattack occurs on an Emergency Operations Center (EOC) system, the consequences could be interference with transmissions containing important intel between operators, leading to emergency management personnel not receiving information for dispatch to activate first responders, distribute necessary resources, locate patients, and more (Gilbert et al. 2003). Additionally, water and electricity can be governed by Supervisory Control and Data Acquisition (SCADA) systems. Manipulation of SCADA systems through a cyberattack introduces risks of public health crises or transportation disruptions (Gilbert et al. 2003), which can further impede emergency operations. Attacks on these integral, interconnected components can create obstacles for emergency management when dealing with natural disasters, complicating the challenges faced by leadership, operators, and affected communities.

Emergency management is reliant on cyber-protected infrastructure, but there is still not sufficient comprehension of how to deal with the complexities of this system in relation to cybersecurity concerns (Walker 2012). Therefore, it is important to continuously examine how critical infrastructure (such as emergency services) can be safeguarded from cyber threats, particularly when they occur concurrently with natural disasters. Since disruptions in one infrastructure sector can greatly affect another, ongoing exploration into shielding critical infrastructure from these threats is essential. Developing and implementing new approaches is crucial to actively address these concerns and enhance preventive measures.

Related Research

Protecting Critical Infrastructure

Taking action to mitigate threats of all kinds is imperative to protecting critical infrastructure. Some of the first federal research efforts were by the President's Commission on Critical Infrastructure Protection (PCCIP), exploring vulnerabilities of eight specific infrastructures (e.g., emergency services, telecommunications, transportation, and others), to curate strategies to improve security and develop plans (Pikus 2003). Since those efforts, more progress has been made to create more approaches for defending against threats, both physical and cyber, to such necessary systems in society. Probabilistic risk models for critical infrastructure are commonly used for enhanced reliability assessment (Tien and Der Kiureghian 2017), deterioration and condition status (Saeed et al. 2017), and vulnerabilities that affect widely utilized networks (Hosseini Nourzad and Pradhan 2016). They are also used to assess infrastructure interdependencies, including physical and cyber components, to increase resiliency and reduce damage from events (Johansen and Tien 2018) or analyze interconnectedness to other infrastructure for decision-making under various scenarios (Ezell et al. 2000). Other research has also analyzed the interdependencies of critical infrastructure using optimization models to detect damage to human-machine interface systems when a natural disaster or a cyberattack occurs (Baycik and Sharkey 2019).

Additional approaches to protecting critical infrastructure include optimization-based simulation and scenario-based methods to show operations during a disaster (Arboleda et al. 2009) and to determine research and development (R&D) priorities (Hamilton et al. 2013). Game theory and network science have also been used to address problems faced when defending against attacks (Sun et al. 2023). In recent years Natural Language Processing (NLP) and text mining have been performed to determine risks to infrastructure. For instance, Jallan and Ashuri (2020) extracted information from construction reports to classify documents into appropriate risk types impacting the construction field. Chowdhury and Zhu (2023) utilized topic modeling to identify topics in transportation infrastructure that affect its planning. While methods such as risk modeling and optimization have been studied greatly to protect critical infrastructure in the engineering domain, there are limited studies that utilize the computational tools of NLP and text mining methods to analyze potential risks to these systems. Some studies address effects of a natural or man-made disruption on critical infrastructure; however, more studies are needed to address when both occur together.

NLP for Cybersecurity

One common use of NLP is human language emulation. NLP can execute tasks such as extracting information from unstructured data (e.g., text) and is used in applications of cybersecurity (Ukwen and Karabatak 2021). NLP began to be utilized in cybersecurity research because most current approaches to detect or predict cyberattacks, current and past, have been shown to be manual (i.e., time-consuming) and costly (Kuhl et al. 2007). Additionally, models can assume that all attack steps can be performed instantly, not including multiple paths or relationships between attack techniques (Xiong et al. 2022). To meet the challenge of more quickly and efficiently identifying cyber threats, studies have been completed using NLP techniques to create both word and phrase embeddings for the cybersecurity domain to use in modeling (Purba et al. 2020; Ranade et al. 2021), to employ automated techniques for analysis of cybersecurity text to uncover understanding of threats (Trong et al. 2020), to analyze sentiments from cybersecurity reports (Phandi et al. 2018), and to develop semi-supervised models for security entity extraction (Jones et al. 2015). These approaches in turn can aid in better detection of cyberattacks, through augmented comprehension and prediction of potential scenarios. NLP can be used in cybersecurity overall for subjects such as malware detection, threat intelligence, privacy preservation, vulnerability exposure, and more (Ukwen and Karabatak 2021).

Research has further explored the use of NLP with two prominent knowledge bases in the cybersecurity domain, MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. MITRE ATT&CK is a foundational knowledge base that focuses on computer information networks and can be used for the development of models related to phases of an adversary attack (Strom et al. 2018). Studies have been executed with MITRE ATT&CK to create graph databases with multiple cyber-based documents (Pelofske et al. 2023), to extract temporal relationships between actions and artifacts from threat reports to detect cyber behaviors (Husari et al. 2019), and to map software vulnerabilities to techniques with neural networks (Kuppa et al. 2021). Additionally, NLP has been used to advance attack graphs by mapping them to MITRE ATT&CK Enterprise Matrix techniques using term frequency-inverse document frequency (TF-IDF) and cosine similarity to authenticate adversarial actions (Haque et al. 2023). Implementing MITRE ATT&CK

allows researchers and industry personnel to better understand threats and patterns to connect tactics, techniques, and procedures (TTPs). This enhanced comprehension can lead to increased mitigation of malicious cyber behaviors and risks through additional insight and situational awareness needed for defense against attackers.

Widely adopted, the NIST Cybersecurity Framework is designed to help mitigate risks associated with cyber threats (NIST 2023). The NIST Cybersecurity Framework has had few studies that apply NLP-based approaches. However, research done with this framework entails using it to generate models to evaluate compliance levels (Teodoro et al. 2015) or security of organizations (Udroiu et al. 2022), develop new frameworks of resilience for proper management of infrastructure (Belalcázar et al. 2017), and to compare it against other standards and frameworks (Syafrizal et al. 2020) or propose new security maturity models (Almuhammadi and Alsaleh 2017). The NIST Cybersecurity Framework is noted though to not be a one-size-fits-all approach for organizations (i.e., not comprehensive to address all cybersecurity processes) (Almuhammadi and Alsaleh 2017). Therefore, adding additional threat data would strengthen the application of this framework. Combining information from both knowledge bases for critical infrastructure analysis, Kwon et al. (2020) developed a cyber threat dictionary manually linking threat actors' attack tactics from the MITRE ATT&CK ICS Matrix to controls from the Facility Cybersecurity Framework (based on the NIST Cybersecurity Framework); however, this method not only relied on manual processes and focused on tactical aspects (i.e., understanding the reasons behind an attack) but also aimed to synchronize defense with each stage of the attack, favoring a more adaptable defense approach. Depending on the nature of the threat, this approach holds its own merits. Yet, a reactive defense (directed against the attack) can be critical in averting immediate damage or halting the attack, particularly in time-sensitive emergency or disaster scenarios. Prioritizing direct action against the ongoing attack, a reactive approach, especially when combined with an automated process emphasizing techniques (i.e., how an attack unfolds), can significantly bolster immediate response capabilities.

Methodology

With technology continuing to advance and the complex digital world evolving, the demand for automated systems is increasing. The gaps in current literature to protect critical infrastructure and use NLP to try to speed the process of analyzing threat related information have led to a limited number of studies for preemptive measures in the following areas: (1) prediction of cyberattacks during simultaneous natural disasters in critical infrastructure sectors, such as the emergency services sector; and (2) incorporation of NLP-based methods for fully automated attack path prediction. Therefore, in this study, to the best of our knowledge, we address these shortcomings and present a novel approach to generate hypothetical cyberattack scenarios (i.e., potential attack paths) employing an automated, NLP-based approach with both cyber-based and emergency management–based context. We also provide suggested preventive measures for the techniques found in the attack paths. We use both the MITRE ATT&CK Enterprise Matrix and the NIST Cybersecurity Framework, as well as the Federal Emergency Management Agency (FEMA) textual information and relevant cybersecurity documents, to achieve this. The attack paths generated show relationships found between techniques in the MITRE ATT&CK Enterprise Matrix. The length of the attack paths spans from shortest to longest path and represent a range of attacker skill levels from script kiddies to top-tier nation states. The techniques are mapped to the NIST Cybersecurity Framework to identify further potential relationships between techniques and protective measures.

Text mining methods are a common multidisciplinary tool used to analyze word-based data and are at the intersection of computational linguistics, artificial intelligence/machine learning, statistics, and information science. NLP has been known to decrease issues that occur with text mining (Talib et al. 2016), and it is common to see both when dealing with textual data. Methods such as NLP have begun to be used in the cybersecurity field for tasks such as analyzing cyber-related documents (Georgescu 2019). The high-level steps taken to execute our study were: collecting the data, transforming the data from unstructured to structured, numerically representing the text, and establishing relationships and discovering patterns between both the techniques and the techniques with protective measures based on semantic similarity. Fig. 1 below shows the workflow of our NLP-based approach in more detail. Ultimately, our approach aims to generate hypothetical attack scenarios intended for integration into a larger system. Its deliberate design revolves around aiding in eventual comprehensive risk mapping, assessing potential consequences like severity and permanence, and evaluating the intricacies involved in executing attacks linked to specific hazards. This approach stands as a pivotal early step to enumerate attack paths in this larger system and to foster the creation of diverse narrative scenarios. These narratives can offer professionals valuable insights into potential system breaches by attackers. Moreover, they expand the range of scarce scenarios available, providing significant learning opportunities for threat prevention strategies. In the remainder of this section, we further explain step-by-step each task executed in our approach.

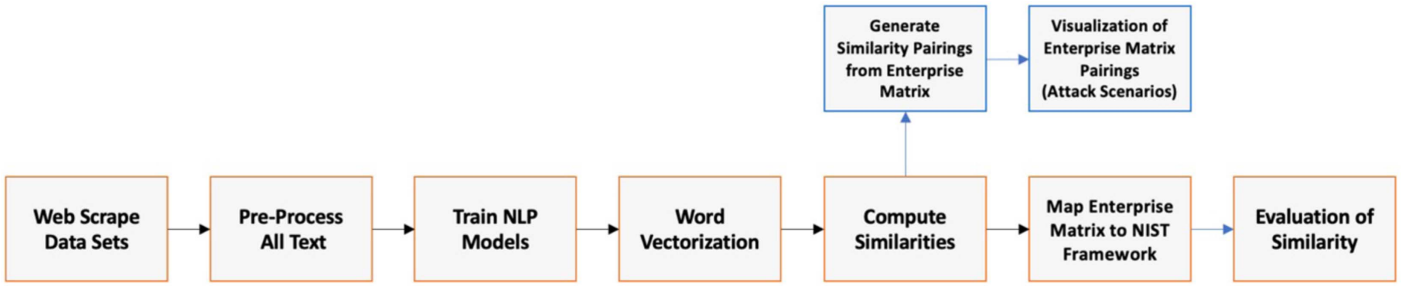

Fig. 1. Our NLP-based framework that automatically generates sets of attack paths from the MITRE ATT&CK Enterprise Matrix's definitions of techniques, with both cyber-based and emergency management–based context; maps techniques to protective measures found in the NIST Cybersecurity Framework to anticipate preemptive solutions; and generates a visualization of the possible attacks.

J. Infrastruct. Syst., 2024, 30(3): 04024008

Data Sets

To execute the objective of our study, four forms of data sets were used. We used data in the form of the pretrained Word2Vec cyber-phrase model (Purba et al. 2020) and textual data from FEMA, MITRE ATT&CK Enterprise Matrix, and the NIST Cybersecurity Framework. We will further describe each data set in more detail in the following sections.

Cyber-Phrase Model

To obtain cybersecurity context, we used the data found in the pretrained model by Purba et al. (2020), which is trained on cybersecurity related material. This is a Word2Vec-based model that produces phrase vectorization of text, and demonstrated that it outperformed word vectorization of the popular, competing models by the IBM-funded UMBC model and Google's model (Purba et al. 2020). These were initially considered prior to discovering the performance of the phrase model. The data itself used to train the model include "CTI reports (Fireeye, Talos, Symantec, APTnotes, SANS, and others), Common Weakness Enumeration (CWE), National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE), MSDN documents, security books, and security papers" (Purba et al. 2020). Using this model, this embedded data was also included in our study for cyber-related information since we employ this model later in the analysis.

FEMA

To get data related to emergency management information on cybersecurity, we utilized news and multimedia written pieces (FEMA 2019, 2020, 2022), a guidance document (FEMA 2009), and an article/information sheet (FEMA 2023) by FEMA. The information discusses material on the impact of cyber threats with emergency management crises, FEMA's adopted goals and objectives, key messages (e.g., risks associated with where a cyberattack could occur, types of cyberattacks, etc.), and preparedness measures. These documents are all used to train the emergency management–based model we construct that will be discussed in a later section.

MITRE ATT&CK Enterprise Matrix

As mentioned prior, one of the leading knowledge bases with cyber-related texts is MITRE ATT&CK. Its core components are tactics, techniques, sub-techniques, documented adversary usage of techniques, and other metadata (Strom et al. 2018). The relationships between the various tactics and techniques can be seen in the matrices. The MITRE ATT&CK Enterprise Matrix in particular represents the most traditional platforms and technologies, including those used in infrastructure systems such as hospitals. The descriptions provided by each technique connect to the tactics and strategies used by an adversary for an attack. Tactics are the "why" of a technique, whereas the technique itself is the "how" an adversary achieves its attack (The MITRE 2023). As this study is most interested in how an attacker can execute a cyber intrusion and looking at critical infrastructure that represents and uses more traditional platforms, the Enterprise Matrix techniques were the proper matrix and information to study. At the time of this analysis, there were 196 techniques in the Enterprise Matrix version used each with paragraph descriptions entailing actions that lead to successful execution. This data is what was used as the techniques in potential attack paths produced.

NIST Cybersecurity Framework

Upon an executive order by former President Barack Obama to improve cybersecurity approaches due to national security, the NIST Cybersecurity Framework was created (Office of the Press Secretary 2013) and has since been commonly implemented into cyber risk management. The NIST Cybersecurity Framework is designed to help mitigate threats associated with cybersecurity (tackling physical, cyber, and people dimensions) made up of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles (NIST 2023). The Framework Core is what this study focuses on, as it contains actions that can be taken and outcomes that can occur with proper prevention. It provides a cyclical process to managing cyber risks with activities related to the functions known as identify, protect, detect, respond, and recover (NIST 2023). Since the goal of this work is to protect critical infrastructure and ensure resources and services are accessible, the protect function of the Framework was utilized, as it has the same objective. This function has six categories: Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology (NIST 2023). These six categories are what the MITRE ATT&CK Enterprise Matrix techniques are mapped to in order to see what potential risk management plans can be used on techniques executed when both a cyber and natural hazard occur.

Web Scrape Data Sets

To obtain the data from FEMA, MITRE ATT&CK, and the NIST Cybersecurity Framework, web scraping was performed to get most of the data used. All three data sources have websites where definitions, documents, etc. are housed. Web scraping is when information is automatically extracted from a website using an algorithm; it takes content from the website and transforms it to be saved in an alternative format, such as a spreadsheet. In our case, we collected and stored the material from the websites into spreadsheets, with each row representing a definition, block of text from a document, description of an action, and so on. The common Python package, BeautifulSoup (Python Package Index 2023), was used to get the desired text from the three websites. Upon web scraping, there were three respective spreadsheets for FEMA, MITRE ATT&CK, and the NIST Cybersecurity Framework with their cybersecurity information.

Preprocess All Text

Textual data is unstructured; therefore, the use of NLP is performed via preprocessing. Standard techniques such as tokenization, stop words removal, stemming, and lemmatization were performed on the text from FEMA, MITRE ATT&CK, and the NIST Cybersecurity Framework, as done in previous studies (Salley et al. 2021). This was done to preprocess the data and transform it so it is prepared to be integrated into a machine learning model. Words with less than three letters were also removed, as well as filtering out words that were not nouns, verbs, adjectives, or that were non-English. When the descriptive text from all three data sources was cleaned, each data set was then a new corpus of only words that fit this criterion.

Train NLP Models

For this study, we have three models: (1) the inclusion of the already pretrained Word2Vec cyber-phrase model for the cyber-based context to pair techniques (Purba et al. 2020) (which is adjusted within means to match the parameters of the other models for similarity score calculation and pairing of techniques), (2) a Doc2Vec model we train on the FEMA data set for emergency management–based context for similarity score calculation and pairing of techniques, and (3) a Doc2Vec model we train on the NIST Cybersecurity Framework's descriptions of protective actions for similarity score calculation and classification of techniques later on.

For the remainder of the paper, these models will be referred to as the Cyber-phrase model, the FEMA Doc2Vec model, and the NIST Doc2Vec model. The Cyber-phrase model established by Purba et al. (2020) uses Word2Vec, which was already embedded into the downloaded model. Doc2Vec was the selected model for the two models we built, as it is an extension of Word2Vec, being able to learn from both word vectors and entire paragraphs to produce numerical representation (Datta et al. 2020). As we are working with textual definitions and multiple sentences, Doc2Vec being able to analyze both words and large portions of text was selected and employed for vectorization. The dimensions for all three models were 100, in alignment with the set dimensions of the cyber-phrase model. For the rest of the parameters in each Doc2Vec model, similar to previous studies, the baseline hyperparameters were utilized (Dogru et al. 2021; Gensim 2022). The entire documents are used to train the Doc2Vec models, as Doc2Vec models are unsupervised without any annotated information, so there is no need to withhold any data for a test set (Lau and Baldwin 2016). After being trained, each model ran an analysis on the MITRE ATT&CK Enterprise Matrix technique definitions, to begin to create embeddings and analyze the similarity of the techniques based on cyber-based and emergency management–based contexts. This is discussed in the coming sections.

Word Vectorization

Upon training the models, we then take the clean corpus of the MITRE ATT&CK Enterprise Matrix technique definitions created during preprocessing and run them through the models to obtain vectorizations of the words in the document. The vectorization process gives numerical value to each word in the corpus, allowing it to be analyzed for semantic similarity based on its values via vector representation. The produced vectors are normalized, so the magnitude of the vectors does not influence the similarity scores created. Note: to train the Doc2Vec models, the FEMA and NIST Cybersecurity Framework also had to be preprocessed and vectorized.

Compute Similarities

Pairwise cosine similarity is a popular, well-established method used in similarity analysis, as it is not affected by the length of each document, but rather by the importance of the words in each document and its high accuracy (Ristanti et al. 2019). Eq. (1) shows how to calculate pairwise cosine similarity, where, if x and y are row vectors, k is their cosine similarity; the Euclidean (L2) normalization projects the vectors on the unit sphere and the dot product finds the degree of similarity through the cosine of the angle between them (scikit learn 2023)

$$k(x, y) = \frac{\boldsymbol{x}\boldsymbol{y}^T}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|} \tag{1}$$

The pairwise cosine similarity scores were calculated for the text run through each model described previously. The cosine similarity was then converted into similarity matrices. Similarity scores were then generated for all possible pairs of the MITRE ATT&CK Enterprise Matrix techniques with the cyber-phrase model and the FEMA Doc2Vec model, for further analysis of the possible technique relationships. The techniques were paired in starting and resulting techniques to visualize their connections and potential pathways (Xiong et al. 2022). The set threshold for the final pairings was 0.5. Despite this threshold seeming relatively conservative, it produces satisfactory results (Zhai et al. 2011) and we wanted to fully maximize the number of pathways possible. To visualize the respective pairings, various subset graphs of paths from the dense networks of all pairings were created, displaying the shortest and longest paths generated from the NLP-based process and the manual process (discussed in detail later), respectively. We define the subset graph of paths as $G(N, A)$ where N is the set of nodes and A is the set of arcs or edges. The nodes in our study are the MITRE ATT&CK Enterprise Matrix technique themselves (i.e., technique names) and the edges represent their similarity score within the set threshold established. When the NLP-based process was initially graphed, very dense networks were created that had realistic portrayals of some nodes circling back to themselves in attempts to try techniques again and that the paths to each technique in this network is not too far from one another. The dense graphs, while too dense for practical output visualization, showed how connected these techniques are, and examining the degrees of the nodes further would show the most prominent techniques used for cyberattacks alone or coinciding with a natural disaster. To illustrate relationships, however, we created figures displaying potential pathways from one node to another, by looking at a real-life scenario. Due to availability, the publicly available cyberattack report we were able to utilize for visualization was on the Ukraine Cyberattack. The attack occurred in 2015 and caused over 3 hours of power outages, affecting nearly 225,000 people (CISA 2021). According to the SANS Industrial Control Systems Library's ICS Defense Use Case report on the incident, there were nine technical components, that were consolidated into six, used by the adversaries (Lee et al. 2016). Pertaining to the MITRE ATT&CK Enterprise Matrix techniques, a critical attack path of this cyberattack began with a spear phishing attachment to enter the system and ended with a system shutdown/reboot to hack the system (Xiong et al. 2022). We ran an analysis on the graph with the starting node as Internal Spearphishing and the resulting node as System Shutdown/Reboot. Our approach (i.e., NLP-based process) was able to generate several alternative attack paths to this starting and resulting technique. Fig. 2(a) illustrates the shortest path (two steps) and Fig. 2(b) illustrates the longest path (71 steps) of these techniques for the NLP-based process. Fig. 3(a) illustrates the shortest path (five steps) and Fig. 3(b) illustrates the longest path (20 steps) of these techniques for the manual process (Xiong et al. 2022). These paths may denote varying levels of attacker expertise, contingent upon the depth of knowledge and resources employed to execute the attack. The NLP-based process demonstrates a broader spectrum of attacker skill levels. This is evident as it accommodates longer longest paths and shorter shortest paths, indicating a more extensive representation of skill variations within the system.

The embeddings or vectorizations of the techniques from these two models were concatenated, representing both cyber and emergency management documentation on threat information, to be mapped to and classified by the NIST Cybersecurity Framework's protective measures.

Map Enterprise Matrix to NIST Framework

The concatenated vectorizations from both the Cyber-phrase and FEMA Doc2Vec models on the MITRE ATT&CK Enterprise Matrix technique definitions were mapped to the outlined "Protect" category via unsupervised classification to the six classes found in this function. The concatenated vectorizations produced 162,111 pairs, creating a graph with 191 nodes and 18,185 edges. Table 1 shows the results, displaying the projected action that can be taken to mitigate each associated technique. In this analysis, according to the similarity scores, five of the six categories were most related to the MITRE ATT&CK Enterprise Matrix techniques (none were mapped to Protective Technology). The absence of the implementation of Protective Technology in this scenario can be justified in

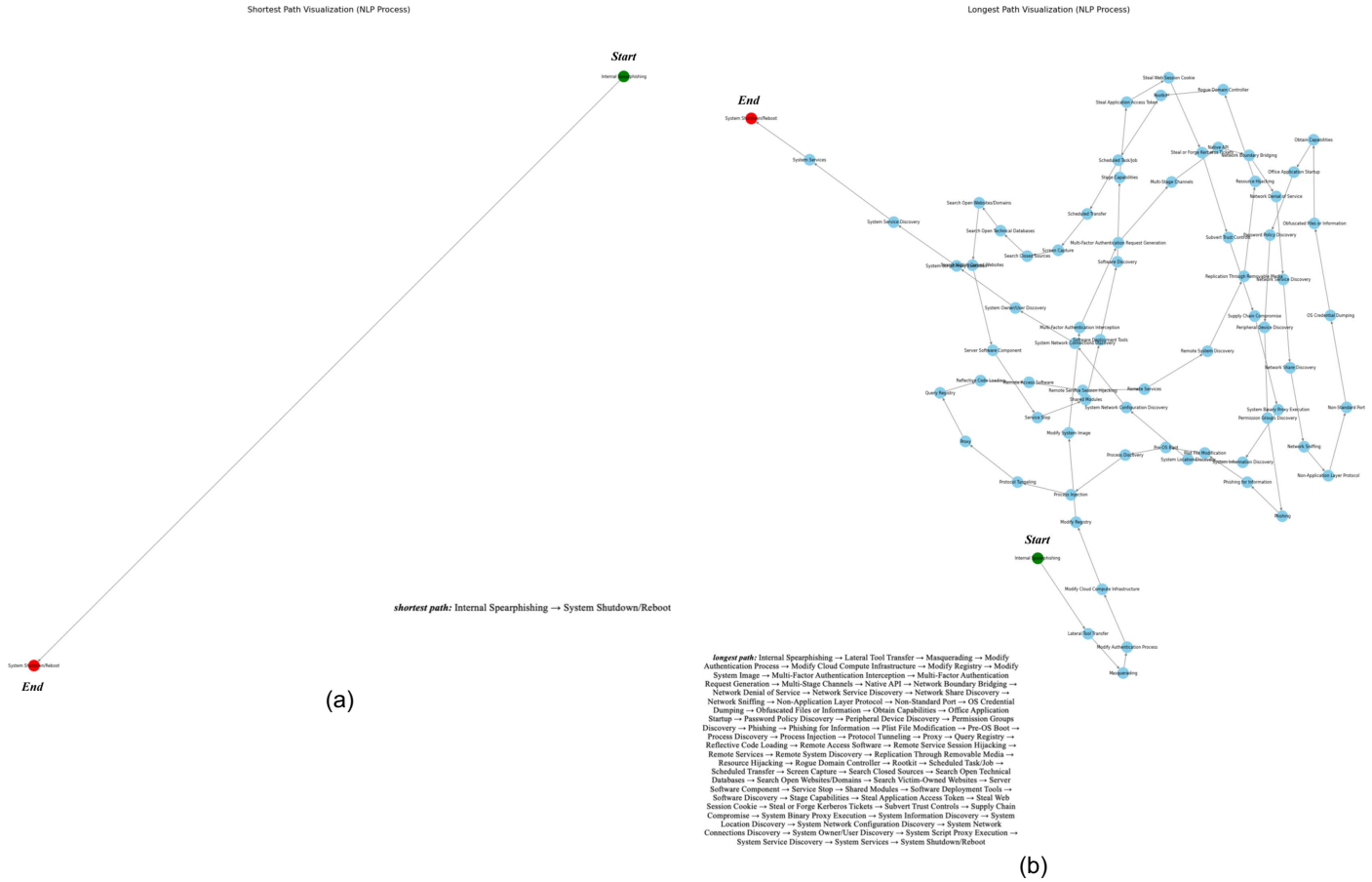

Fig. 2. (a) Shortest path visualization from starting node (annotated with "Start") to ending node (annotated with "End") for the 2015 Ukraine Cyberattack based on the NLP-based process; and (b) longest path visualization from starting node (annotated with "Start") to ending node (annotated with "End") for the 2015 Ukraine Cyberattack based on the NLP-based process.

relation to emergency management and cybersecurity. The lack of techniques aligning with this category could stem from the desire to minimize exposure to further vessels of intrusion, which is a priority for FEMA and other relevant agencies. By avoiding excessive technological devices, the risk of increased vulnerability is further mitigated.

Evaluation of Similarity

To test the validity of the similarity scores produced between the vectors for concatenation and for the classification of techniques to the NIST Cybersecurity Framework "Protect" actions, p-values were calculated to determine the statistical significance or linear relationship between the pairings. Common similarity measures are cosine similarity or Pearson's correlation to measure distance or the relationship between data sets; either can be used, but one must determine which is best for their study. In this study, for its ability to be unaffected by scalar transformations in the data whereas Pearson's similarity measure can (Van Dongen and Enright 2012), cosine similarity was used to measure likeness. With Pearson's being affected by scalar transformations in the data, this can impact its correlation coefficient interpretation, therefore, cosine similarity was the better measure for this reason and its other strengths mentioned in a previous section. The two measures though are mathematically related, being noted Pearson is identical to the cosine being applied in the cosine similarity calculation (Van Dongen and Enright 2012). Given the mathematical relationship between the two, it is noteworthy that while the coefficient may not be the most reliable metric for assessing correlation or similarity, the p-value of Pearson's correlation can be employed to robustly evaluate the significance of cosine similarity. From the Pearson's calculation (The SciPy Community 2023), Table 2 below shows the associated p-value scores between each vector to validate the merging of embeddings and classification process, testing if the vectors have a meaningful relationship.

Based on the p-values, it is evident that the relationship between the cyber-based vectorizations of the technique definitions and the emergency management–based vectorizations of the technique definitions have significant similarity based on the scores produced, in turn validating the execution of combining these two models that are strongly associated to provide further context to the overall goal of protecting both natural and cyber disasters simultaneously. The p-values also validate the classification performed between the concatenated cyber-phrase and FEMA Doc2Vec similarity matrix to the protective actions in the NIST Cybersecurity Framework. Demonstrating the strong relationship between the data sets shows the unsupervised classification (i.e., with no ground truth to perform typical metrics such as F1 or accuracy) is statistically conclusive for being able to assess similarity of the MITRE ATT&CK Enterprise Matrix techniques to generate pairings and select categories for preventive activities. Overall, the low p-values infer that the models are robust and the similarity scores are reliable measures.

Furthermore, to determine if the attack paths created with this NLP approach could generate an equal or greater number of attack

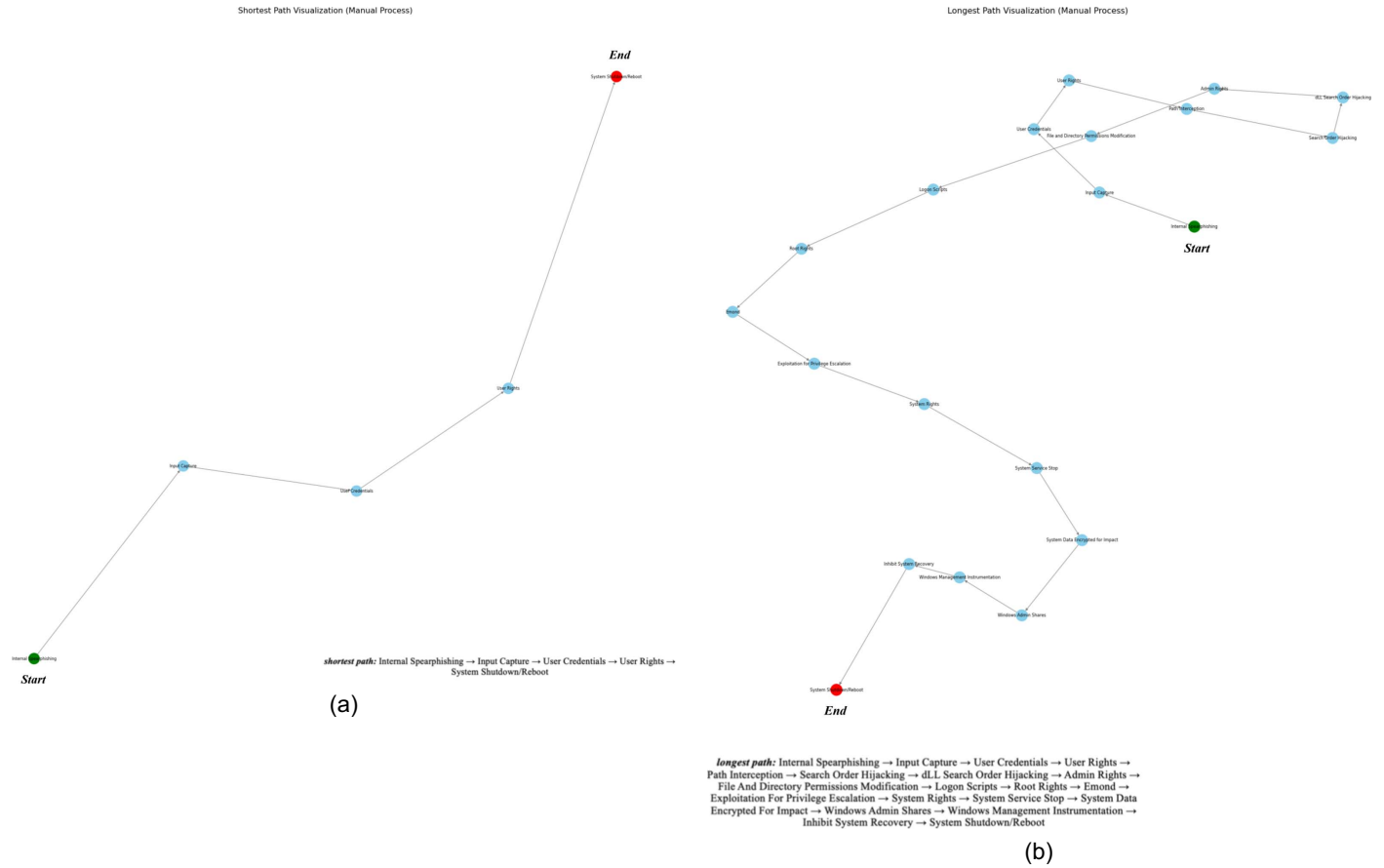

Fig. 3. (a) Shortest path visualization from starting node (annotated with "Start") to ending node (annotated with "End") for the 2015 Ukraine Cyberattack based on the manual process; and (b) longest path visualization from starting node (annotated with "Start") to ending node (annotated with "End") for the 2015 Ukraine Cyberattack based on the manual process.

paths predicted by manual processes and faster in completion (i.e., not taking several hours or days to annotate to determine sequences), we compared the quantity and time of our execution of potential cyberattacks with a previous study that manually generated attack steps with the MITRE ATT&CK Enterprise Matrix as well. Xiong et al. (2022) proposed enterpriseLang based on meta attack language. Through parsing the main enterpriseLang file there were 1,009 pairs of techniques. Manual annotation not only can take significant time to do and requires domain expertise, but there are also challenges with disagreements between annotators (Trong et al. 2020), which can call into question consistency. With our final cyber-based and emergency management–based model, our approach was able to capture 162,111 pairs of potential attack paths in comparison to the manual process and was able to complete this task in a few minutes. Table 3 displays these results.

The manual process could take hours to days to complete with a team of researchers; completing the task in a few minutes and with statistical significance substantially outpaces the manual processing speed.

Discussion

With the digital world progressively growing (e.g., internet usage increasing), cyberattacks will continue to be an imminent risk that society faces, particularly when disasters strike simultaneously that are both natural and human-made. State and local government officials need to implement cybersecurity plans, drills, or workshops for emergency preparedness, so they can properly respond to crisis events and help those in need without the disruption of a cyberattack in their networks, generating more issues to an already heightened event. For instance, in 2021, the state of Indiana's federally funded Multi-State Information Sharing and Analysis Center (which helps protect against cyber threats) participated in exercises to assist them with how to deal with the potential impacts of both a natural disaster and a cyberattack at the same time, and in 2018 the city of Houston and the US Army Cyber Institute hosted a three-day drill on how to handle cyberattacks during a hurricane (Bergal 2021). Efficient training, communication, and regularly updated policies are pertinent to plan for cyberattacks, as well as state-of-the-art systems being in place that can mitigate cyber threats promptly after a major incident occurs that weakens critical infrastructure needed to sustain communities. An approach such as ours can be important across multiple sectors, given the interdependencies of the various types of critical infrastructure.

Our study has practical contributions that can positively impact society. One, our study provides an approach to more quickly and efficiently assess potential cyberattacks. It also aids in protecting critical infrastructure, such as emergency response telecommunications, pertaining to natural disasters when implemented into cyberattack prevention efforts. Also, this work can further aid in mitigating impacts of natural disasters by allowing efficient execution of response efforts without interference in pertinent networks. For instance, in the context of emergency medical services, any disruption in transportation systems could drastically impact response times. For example, one possible scenario could be a hacker

Table 1. The categories found in the "Protect" function in the NIST Cybersecurity Framework and the techniques from the MITRE ATT&CK Enterprise Matrix matched to mitigate based on similarity scores

Category	Techniques
Identity management and access control	Event triggered execution, execution guardrails, exfiltration over, alternative protocol, subvert trust controls, supply chain, compromise, system binary proxy execution, valid accounts
Awareness and training	Abuse elevation control mechanism, access token manipulation, account access removal, acquire infrastructure, active scanning, adversary-in-the-middle, audio capture, automated collection, automated exfiltration, bits jobs, boot or logon autostart execution, boot or logon initialization scripts, browser bookmark discovery, browser extensions, browser session hijacking, brute force, build, image on host, clipboard data, command and scripting interpreter, communication through removable media, compromise accounts, compromise client software binary, compromise infrastructure, credentials from password stores, data destruction, data encoding, data encrypted for impact, data manipulation, data from configuration repository, data from information repositories, data from local system, data from network shared drive, data from removable media, debugger evasion, defacement, establish accounts, event triggered execution, exfiltration over C2 channel, exfiltration over other, network medium, exfiltration over physical medium, exfiltration over web service, exploit public-facing application, exploitation for client execution, exploitation for credential access, exploitation for defense evasion, forge web credentials, gather victim host information, gather victim identity information, gather victim network information, hide artifacts, hijack execution flow, impair defenses, implant internal image, indicator removal on host, input capture, inter-process communication, internal spearphishing, lateral tool transfer, masquerading, modify cloud compute infrastructure, modify registry, modify system image, multi-factor authentication interception, multi-factor authentication request generation, multi-stage channels, native API, network boundary bridging, OS credential dumping, obfuscated files or information, office application startup, password policy discovery, peripheral device discovery, permission groups discovery, phishing, phishing for information, process discovery, process injection, remote service session hijacking, remote services, remote system discovery, replication through removable media, resource hijacking, search closed sources, search open technical databases, search open websites/domains, search Victim-owned websites, server software component, stage capabilities, steal application access token, steal web session cookie, steal or forge Kerberos tickets, subvert trust controls, system binary proxy execution, system services, system shutdown/reboot, system time discovery, taint shared content, template injection, traffic signaling, transfer data to cloud account, trusted developer utilities proxy execution, trusted relationship, unsecured credentials, use alternate authentication material, user execution, valid accounts, video capture, virtualization/sandbox evasion, weaken encryption, web service, windows management instrumentation, disk wipe, domain policy modification, domain trust discovery, drive-by compromise, dynamic resolution, email collection, modify authentication process, rogue domain controller, rootkit, scheduled task/job, scheduled transfer, screen capture, encrypted channel, endpoint denial of service, escape to host
Data security	System information discovery, system location discovery, system network configuration discovery, system network connections discovery, system owner/user discovery, system script proxy execution, system service discovery, system services, compromise infrastructure, container administration command, container and resource discovery, create account, create or modify system process, use alternate authentication material
Information protection processes and procedures	Cloud infrastructure discovery, cloud service dashboard, cloud service discovery, cloud storage object discovery, command and scripting interpreter, process injection, protocol tunneling, proxy, query registry, reflective code loading, remote access software, remote service session hijacking, unused/unsupported cloud regions, XSL script processing, phishing for information, phishing, plist file modification, pre-OS boot, web service, boot or logon autostart execution, boot or logon initialization scripts, unsecured credentials, network boundary bridging, network denial of service, network service discovery, network share discovery, network sniffing, non-application layer protocol, non-standard port, OS credential dumping, weaken encryption, data manipulation, data obfuscation, data staged, data transfer size limits, data from cloud storage object, use alternate authentication material, indicator removal on host, indirect command execution, ingress tool transfer, inhibit system recovery, input capture, obfuscated files or information, obtain capabilities, office application startup, server software component, service Stop, shared modules, software deployment tools, software discovery, stage capabilities, virtualization/sandbox evasion, account discovery, account manipulation, acquire infrastructure, defacement, deobfuscate/decode files or information, deploy container, develop capabilities, direct volume access, disk wipe, gather victim network information, gather victim org information, group policy discovery, hardware additions, user execution, valid accounts
Maintenance	Adversary-in-the-middle, application layer protocol, application window discovery, archive collected data, exploitation for privilege escalation, exploitation of remote services, external remote services, fallback channels, file and directory discovery, file and directory permissions modification, firmware corruption, forced authentication, forge web credentials, unsecured credentials, valid accounts

Table 2. Significance of the similarity pairings generated by each model

Vector X	Vector Y	p-value
Cyber-Phrase similarity matrix	FEMA Doc2Vec similarity matrix	<0.05
Cyber-Phrase & FEMA Doc2Vec concatenated similarity matrix	NIST Doc2Vec similarity matrix	<0.05

Table 3. Comparison of automated versus manual process for quantity of technique pairings output

Graph element	NLP process (combined cyber-based and emergency management–based models)	Manual process (Xiong et al. 2022)
Nodes	191	397
Edges	18,185	904
Pairs	162,111	1,009

interfering with traffic signals or sensors, causing congestion or potentially fatal accidents (Chowdhury and Zhu 2023). This disruption would inevitably lead to delays in response times by first responders, compromising patient stability, escalating the risk of loss of life, or depriving individuals of timely medical attention, intensifying the severity of the situation. Approaches such as the one introduced in this paper can be used to alleviate such scenarios and possibly prevent such obstacles in these critical infrastructure sectors. To the domain of research related to protecting critical infrastructure and emergency management, the study lays the foundation for the need for more advanced NLP processes to generate attack scenarios (Ukwen and Karabatak 2021). And it also is an approach on how to ensure emergency response is not impeded by cyberattacks (Loukas et al. 2013). To the best of our knowledge, this study is also one of the first to create an NLP-based model to generate cyberattacks that considers both the cyber-based and emergency management–based context, representing both human-made and natural disasters in the model.

Furthermore, with this study producing hypothetical scenarios, there is a possibility that the combinations of pairs based on similarities and the multiple paths they generate could create zero-day or unknown attack paths (Sejr et al. 2020). This can be further studied going forward to see if this approach generates attack scenarios not seen before. There is no single solution to protect against all zero-day attacks, known or otherwise (Ahmad et al. 2023). Therefore, this study could also contribute to the possibility of methods that can be used to find more zero-day attacks, then develop preventive measures for if they occur. Additionally, our study primarily delved into understanding the methods by which an adversary can execute an attack (i.e., techniques), rather than reasons behind the use of an ATT&CK technique (i.e., tactics). However, upon deeper analysis, we uncovered that all 14 tactics within the MITRE ATT&CK Enterprise Matrix are encompassed by the techniques identified through our pairing approach. This opens avenues for subsequent studies aimed at uncovering additional relationships between these tactics and techniques, potentially facilitating classification or other NLP-based analyses. In general, this study can play a part in overall risk and vulnerability assessments. Such assessments need threat information and technologies that can contain attacks to be included in its process in order to revise and improve mitigation plans (Pikus 2003). Approaches such as ours lead to being able to answer the questions of what can go wrong or what can be done when analyzing such risks (Ezell et al. 2000).

While this study demonstrated a quicker and more effective way to generate potential cyberattacks, there are some limitations to this study. One limitation is the scarcity of publicly available reports on actual cyberattacks, primarily due to privacy concerns, which restricts access for analysis but impedes learning opportunities for hackers. This in turn makes researching actual cases or implementation of effective countermeasures difficult. Constant evolution and advancement of hackers pose another limitation to this study. As this system develops to produce more cyberattack scenarios, if hackers got ahold of this information, they could then plan out how they might be stopped and mitigate around the preventive measures further. As NLP and text mining for cybersecurity continue to develop, there should be a larger discussion around what data, models, or code need to be more confidential versus shared. Cyberattacks are also rarely identical in nature. Therefore, in order to use this framework new text and definitions should be added as a future work. Additionally, while the data sets used were able to capture a good number of relationships between techniques, there are still more, and this is not a comprehensive list of all possible attack paths. It is, though, a step toward the NLP-based automation of these time intensive efforts. Also, more qualitative measures can be taken to evaluate future works as well. While internal and external validation in terms of team discussion and cross-referencing with literature has been seen in NLP (Chowdhury and Zhu 2023), the next step would be surveying cybersecurity working professionals. Similar to other related studies, expert opinion can be incorporated on the paths generated to further determine usefulness in the industry setting (Jallan and Ashuri 2020). Lastly, as with any language-based model there is concern for "hallucination" from the model, or outputs containing errors or inconsistencies with reality. As more active approaches are being generated to detect potential hallucinations broadly in various NLP-based tasks (Ji et al. 2023), the next pivotal phase involves delving into potential instances of hallucination themselves. Future work should analyze and better understand these anomalies, exploring their existence and analyzing how these hypothetical scenarios might diverge from real-world feasibility and impact the effectiveness of our demonstrated approach. Automated approaches to streamline processes reduce potential discrepancies in the annotation process among annotators, improve efficiency through enabling the forecasting of potential cyberattacks more quickly, and identify more paths than the annotated process would produce. However, striking a balance between automated processes and industry conversations that maximize efficiency, accuracy, and cost-effectiveness, while also considering factors such as data volume, complexity, and criticality, would best benefit cybersecurity analyses going forward.

Conclusion

Protecting critical infrastructure from cyberattacks is an important societal issue that affects various sectors from economics to public health. Vulnerability of cyber emergency response is not a new issue (Jennex 2007). However, it is very difficult to protect systems from cyberattacks as they occur, which is why it is important to be able to anticipate and predict what an adversary might do to be able to better mitigate on the front end and reduce such security events (Han et al. 2019). To minimize the threat of cyberattacks, models have been generated to simulate potential cyber threats. Yet, the issue with most current approaches is that they are time-consuming and there can be inconsistencies with the annotation (e.g., consistent reproducibility). In this paper, we proposed an approach that incorporated NLP and text mining to automatically and systematically generate sets of attack paths from the technique descriptions in the MITRE ATT&CK Enterprise Matrix. The study ingested attack-related definitions, produced linkages between techniques, created an output that shows the relationship between techniques and the potential pathways an adversary can take to enact their desired consequence(s), and provided possible protective measures that can be taken. This process is a step toward further protecting critical infrastructure, particularly within the emergency services sector and during natural disasters, when communities are at their most vulnerable. Mitigating the risk of additional attacks,

such as data breaches, during a natural disaster is crucial for enhancing community resilience in such circumstances.

While the focus is on using such generated scenarios to protect critical infrastructure during disasters, this work can complement all parts in both the cyclical process of the four phases of emergency management (i.e., mitigation, preparedness, response, and recovery), and potentially all key functions of the NIST Cybersecurity Framework to enhance cybersecurity awareness and manage risk. Our study emphasizes the urgency of using protective measures against cyberattacks during natural disasters as it is a rising concern. The implementation of proper cybersecurity planning and mitigation strategies for emergency preparedness and response to crisis events can help those in need and reduce unnecessary interference in people's routines or lives caused by cyberattacks. Protecting critical infrastructure from cyber threats directly aids community resilience efforts to better protect society. With stronger community resilience, society will be able to recover faster from crisis events, such as natural hazards and disasters.

Data Availability Statement

Some data, models, or code that support the findings of this study are available from the corresponding author upon reasonable request. The data, models, and code used to create the hypothetical scenarios and pairings can be made available.

Acknowledgments

The preliminary works of this study was conducted in collaboration with Mike Nygaard, Deputy Associate Program Leader, Cyber Modeling & Simulation at Lawrence Livermore National Laboratory during an internship the first author had. This material is based upon work supported by the National Science Foundation under Grant No. 1837021. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or the Lawrence Livermore National Laboratory.

References

Ahmad, R., I. Alsmadi, W. Alhamdani, and L. A. Tawalbeh. 2023. "Zero-day attack detection: A systematic literature review." *Artif. Intell. Rev.* 56 (10): 10733–10811. https://doi.org/10.1007/s10462-023-10437-z.

Almuhammadi, S., and M. Alsaleh. 2017. "Information security maturity model for NIST cyber security framework." *Comput. Sci. Inf. Technol.* 7 (3): 51–62.

Arboleda, C. A., D. M. Abraham, J.-P. P. Richard, and R. Lubitz. 2009. "Vulnerability assessment of health care facilities during disaster events." *J. Infrastruct. Syst.* 15 (3): 149–161. https://doi.org/10.1061/(ASCE)1076-0342(2009)15:3(149).

Argaw, S. T., et al. 2020. "Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks." *BMC Med. Inform. Decis. Making* 20 (Dec): 1–10. https://doi.org/10.1186/s12911-020-01161-7.

Baycik, N. O., and T. C. Sharkey. 2019. "Interdiction-based approaches to identify damage in disrupted critical infrastructures with dependencies." *J. Infrastruct. Syst.* 25 (2): 04019013. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000487.

Belalcázar, A., M. Ron, J. Díaz, and L. Molinari. 2017. "Towards a strategic resilience of applications through the NIST cybersecurity framework and the strategic alignment model (SAM)." In *Proc., 2017 Int. Conf. on Information Systems and Computer Science (INCISCOS)*, 181–187. New York: IEEE.

Bergal, J. 2021. "Natural disasters can set the stage for cyberattacks." Accessed March 2, 2023. https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/10/25/natural-disasters-can-set-the-stage-for-cyberattacks.

Bolton, F. 2013. "Cybersecurity and emergency management: Encryption and the inability to communicate." *J. Homeland Security Emerg. Manage.* 10 (1): 379–385. https://doi.org/10.1515/jhsem-2012-0038.

Chowdhury, S., and J. Zhu. 2023. "Investigation of critical factors for future-proofed transportation infrastructure planning using topic modeling and association rule mining." *J. Comput. Civ. Eng.* 37 (1): 04022044. https://doi.org/10.1061/(ASCE)CP.1943-5487.0001059.

CISA (Cybersecurity & Infrastructure Security Agency). 2021. "Cyber-attack against Ukrainian critical infrastructure." Accessed March 3, 2023. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

CISA (Cybersecurity & Infrastructure Security Agency). 2023. "Critical infrastructure sectors." Cybersecurity & Infrastructure Security Agency. Accessed July 12, 2023. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

Datta, P., N. Lodinger, A. S. Namin, and K. S. Jones. 2020. "Cyber-attack consequence prediction." Preprint, submitted December 1, 2020. http://arxiv.org/abs/2012.00648.

Dogru, H. B., S. Tilki, A. Jamil, and A. A. Hameed. 2021. "Deep learning-based classification of news texts using doc2vec model." In *Proc., 2021 1st Int. Conf. on Artificial Intelligence and Data Analytics (CAIDA)*, 91–96. New York: IEEE.

Ezell, B. C., J. V. Farr, and I. Wiese. 2000. "Infrastructure risk analysis model." *J. Infrastruct. Syst.* 6 (3): 114–117. https://doi.org/10.1061/(ASCE)1076-0342(2000)6:3(114).

FEMA. 2009. "Cyber security guidance." FEMA. Accessed July 13, 2023. https://www.fema.gov/pdf/government/grant/hsgp/fy09_hsgp_cyber.pdf.

FEMA. 2019. "Building a culture of cyber preparedness." FEMA. Accessed July 13, 2023. https://www.fema.gov/blog/building-culture-cyber-preparedness.

FEMA. 2020. "10 tips to know: #BeCyberSmart to be cyber secure." FEMA. Accessed July 13, 2023. https://www.fema.gov/press-release/20230503/10-tips-know-becybersmart-be-cyber-secure.

FEMA. 2022. "Fiscal year 2022 state and local cybersecurity grant program fact sheet." FEMA. Accessed July 13, 2023. https://www.fema.gov/fact-sheet/fiscal-year-2022-state-and-local-cybersecurity-grant-program-fact-sheet.

FEMA. 2023. "Be prepared for a cyberattack." FEMA | Preparedness Community. Accessed July 13, 2023. https://community.fema.gov/ProtectiveActions/s/article/Cyberattack.

Gensim. 2022. "models.doc2vec–Doc2vec paragraph embeddings." Gensim topic modelling for humans. Accessed July 13, 2023. https://radimrehurek.com/gensim/models/doc2vec.html.

Georgescu, T. M. 2019. "Machine learning based system for semantic indexing documents related to cybersecurity." *Econ. Inf.* 19 (1): 5–13. https://doi.org/10.12948/ei2019.01.01.

Gilbert, P. H., J. Isenberg, G. B. Baecher, L. T. Papay, L. G. Spielvogel, J. B. Woodard, and E. V. Badolato. 2003. "Infrastructure issues for cities–Countering terrorist threat." *J. Infrastruct. Syst.* 9 (1): 44–54. https://doi.org/10.1061/(ASCE)1076-0342(2003)9:1(44).

Grigg, N. S. 2003. "Water utility security: Multiple hazards and multiple barriers." *J. Infrastruct. Syst.* 9 (2): 81–88. https://doi.org/10.1061/(ASCE)1076-0342(2003)9:2(81).

Hamilton, M. C., J. H. Lambert, J. M. Keisler, F. H. Holcomb, and I. Linkov. 2013. "Research and development priorities for energy islanding of military and industrial installations." *J. Infrastruct. Syst.* 19 (3): 297–305. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000133.

Han, C. H., S. T. Park, and S. J. Lee. 2019. "The enhanced security control model for critical infrastructures with the blocking prioritization process to cyber threats in power system." *Int. J. Crit. Infrastruct. Prot.* 24 (Mar): 1–13. https://doi.org/10.1016/j.ijcip.2018.10.009.

Haque, M. A., S. Shetty, C. A. Kamhoua, and K. Gold. 2023. "Adversarial technique validation & defense selection using attack graph & ATT&CK Matrix." In *Proc., 2023 Int. Conf. on Computing, Networking and Communications (ICNC)*, 181–187. New York: IEEE.

Hosseini Nourzad, S. H., and A. Pradhan. 2016. "Vulnerability of infrastructure systems: Macroscopic analysis of critical disruptions on road networks." *J. Infrastruct. Syst.* 22 (1): 04015014. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000266.

Husari, G., E. Al-Shaer, B. Chu, and R. F. Rahman. 2019. "Learning APT chains from cyber threat intelligence." In *Proc., 6th Annual Symp. on Hot Topics in the Science of Security*, 1–2. New York: Association for Computing Machinery.

Jallan, Y., and B. Ashuri. 2020. "Text mining of the securities and exchange commission financial filings of publicly traded construction firms using deep learning to identify and assess risk." *J. Constr. Eng. Manage.* 146 (12): 04020137. https://doi.org/10.1061/(ASCE)CO.1943-7862.0001932.

Janczewski, L., and A. Colarik, eds. 2007. *Cyber warfare and cyber terrorism*. Hershey, PA: IGI Global.

Jennex, M. E. 2007. "Modeling emergency response systems." In *Proc., 2007 40th Annual Hawaii Int. Conf. on System Sciences (HICSS'07)*, 1–8. New York: IEEE.

Ji, Z., N. Lee, R. Frieske, T. Yu, D. Su, Y. Xu, E. Ishii, Y. J. Bang, A. Madotto, and P. Fung. 2023. "Survey of hallucination in natural language generation." *ACM Comput. Surv.* 55 (12): 1–38. https://doi.org/10.1145/3571730.

Johansen, C., and I. Tien. 2018. "Probabilistic multi-scale modeling of interdependencies between critical infrastructure systems for resilience." *Sustainable Resilient Infrastruct.* 3 (1): 1–15. https://doi.org/10.1080/23789689.2017.1345253.

Jones, C. L., R. A. Bridges, K. M. Huffer, and J. R. Goodall. 2015. "Towards a relation extraction framework for cyber-security concepts." In *Proc., 10th Annual Cyber and Inf. Security Research Conf.*, 1–4. New York: Association for Computing Machinery.

Kuhl, M. E., M. Sudit, J. Kistner, and K. Costantini. 2007. "Cyber attack modeling and simulation for network security analysis." In *Proc., 2007 Winter Simulation Conf.*, 180–1188. New York: IEEE.

Kuppa, A., L. Aouad, and N. A. Le-Khac. 2021. "Linking cve's to mitre att&ck techniques." In *Proc., 16th Int. Conf. on Availability, Reliability and Security*, 1–12. New York: Association for Computing Machinery.

Kwon, R., T. D. Ashley, J. E. Castleberry, P. L. McKenzie, and S. N. G. Gourisetti. 2020. "Cyber threat dictionary using mitre attack matrix and nist cybersecurity framework mapping." *In Proc., IEEE Resilience Week (RWS 2020) Conf.* New York: IEEE.

Lau, J. H., and T. Baldwin. 2016. "An empirical evaluation of doc2vec with practical insights into document embedding generation." Preprint, submitted July 19, 2016. http://arxiv.org/abs/1607.05368.

Lee, R. M., M. J. Assante, and T. Conway. 2016. "Analysis of the cyber attack on the Ukrainian power grid." *Electr. Inf. Sharing Anal. Center* 388 (1–29): 1–29.

Li, J., Q. Li, C. Liu, S. U. Khan, and N. Ghani. 2014. "Community-based collaborative information system for emergency management." *Comput. Oper. Res.* 42 (Mar): 116–124. https://doi.org/10.1016/j.cor.2012.03.018.

Loukas, G., D. Gan, and T. Vuong. 2013. "A review of cyber threats and defence approaches in emergency management." *Future Internet* 5 (2): 205–236. https://doi.org/10.3390/fi5020205.

NIST. 2023. "Quick start guide." Accessed May 1, 2023. https://www.nist.gov/cyberframework/getting-started/quick-start-guide.

Office of the Press Secretary. 2013. "Executive order–Improving critical infrastructure cybersecurity." Accessed April 30, 2023. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Pelofske, E., L. M. Liebrock, and V. Urias. 2023. "Cybersecurity Threat hunting and vulnerability analysis using a Neo4j graph database of open source intelligence." Preprint, submitted January 27, 2023. http://arxiv.org/abs/2301.12013.

Phandi, P., A. Silva, and W. Lu. 2018. "SemEval-2018 task 8: Semantic extraction from CybersecUrity REports using natural language processing (SecureNLP)." In *Proc., 12th Int. Workshop on Semantic Evaluation*, 697–706. Kerrville, TX: Association for Computational Linguistics.

Pikus, I. M. 2003. "Critical infrastructure protection: Are we there yet?" *J. Infrastruct. Syst.* 9 (1): 1–5. https://doi.org/10.1061/(ASCE)1076-0342(2003)9:1(1).

Ponemon, I. 2016. *Sixth annual benchmark study on privacy & security of healthcare data*. Traverse City, MI: Ponemon Institute.

Purba, M. D., B. Chu, and E. Al-Shaer. 2020. "From word embedding to cyber-phrase embedding: Comparison of processing cybersecurity texts." In *Proc., 2020 IEEE Int. Conf. on Intelligence and Security Informatics (ISI)*, 1–6. New York: IEEE.

Python Package Index. 2023. "Beautifulsoup4 4.12.2." PyPI. Accessed July 11, 2023. https://pypi.org/project/beautifulsoup4/.

Ranade, P., A. Piplai, A. Joshi, and T. Finin. 2021. "CyBERT: Contextualized embeddings for the cybersecurity domain." *In Proc., 2021 IEEE Int. Conf. on Big Data (Big Data)*, 3334–3342. New York: IEEE.

Ristanti, P. Y., A. P. Wibawa, and U. Pujianto. 2019. "Cosine similarity for title and abstract of economic journal classification." *In Proc., 2019 5th Int. Conf. on Science in Information Technology (ICSITech)*, 123–127. New York: IEEE.

Saeed, T. U., Y. Qiao, S. Chen, K. Gkritza, and S. Labi. 2017. "Methodology for probabilistic modeling of highway bridge infrastructure condition: Accounting for improvement effectiveness and incorporating random effects." *J. Infrastruct. Syst.* 23 (4): 04017030. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000389.

Salley, C., N. Mohammadi, and J. E. Taylor. 2021. "Semi-supervised machine learning framework for fusing georeferenced data from social media and community-driven applications." In *Proc., Computing in Civil Engineering 2021*, 114–122. Reston, VA: ASCE.

scikit learn. 2023. "6.8. Pairwise metrics, affinities and kernels." Scikit. Accessed July 11, 2023. https://scikit-learn.org/stable/modules/metrics.html#cosine-similarity.

Seba, A., N. Nouali-Taboudjemat, N. Badache, and H. Seba. 2019. "A review on security challenges of wireless communications in disaster emergency response and crisis management situations." *J. Netw. Comput. Appl.* 126 (Mar): 150–161. https://doi.org/10.1016/j.jnca.2018.11.010.

Sejr, J. H., A. Zimek, and P. Schneider-Kamp. 2020. "Explainable detection of zero day web attacks." In *Proc., 2020 3rd Int. Conf. on Data Intelligence and Security (ICDIS)*, 71–78. New York: IEEE.

Strom, B. E., A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas. 2018. *MITRE ATT&CK: Design and philosophy.* Bedford, MA: The MITRE.

Sun, J., S. Wang, J. Zhang, and Q. Dong. 2023. "Attack–Defense game in interdependent networks: A functional perspective." *J. Infrastruct. Syst.* 29 (3): 04023020. https://doi.org/10.1061/JITSE4.ISENG-2259.

Sutedi, A., E. Gunadhi, D. Heryanti, and R. Setiawan. 2021. "Data privacy in disaster situation: A review." In *Proc., 2021 Int. Conf. on ICT for Smart Society (ICISS)*, 1–4. New York: IEEE.

Syafrizal, M., S. R. Selamat, and N. A. Zakaria. 2020. "Analysis of cybersecurity standard and framework components." *Int. J. Commun. Networks Inf. Secur.* 12 (3): 417–432. https://doi.org/10.17762/ijcnis.v12i3.4817.

Talib, R., M. K. Hanif, S. Ayesha, and F. Fatima. 2016. "Text mining: Techniques, applications and issues." *Int. J. Adv. Comput. Sci. Appl.* 7 (11): 414–418. https://doi.org/10.14569/IJACSA.2016.071153.

Teodoro, N., L. Gonçalves, and C. Serrão. 2015. "NIST cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements." In *Proc., 2015 IEEE Trustcom/BigDataSE/ISPA*, 418–425. New York: IEEE.

The MITRE. 2023. "Enterprise matrix." MITRE | ATT&CK®. Accessed July 13, 2023. https://attack.mitre.org/matrices/enterprise/.

The SciPy Community. 2023. "scipy.stats.pearsonr." scipy.stats.pearsonr-SciPy v1.11.1 Manual. Accessed July 12, 2023. https://docs.scipy.org/doc/scipy/reference/generated/scipy.stats.pearsonr.html.

Tien, I., and A. Der Kiureghian. 2017. "Reliability assessment of critical infrastructure using Bayesian networks." *J. Infrastruct. Syst.* 23 (4): 04017025. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000384.

Trong, H. M. D., D. T. Le, A. P. B. Veyseh, Nguyễn, T., and T. H. Nguyen. 2020. "Introducing a new dataset for event detection in cybersecurity texts." In *Proc., 2020 Conf. on Empirical Methods in Natural Language*

Processing (EMNLP), 5381–5390. Kerrville, TX: Association for Computational Linguistics.

Udroiu, A. M., M. Dumitrache, and I. Sandu. 2022. "Improving the cybersecurity of medical systems by applying the NIST framework." In *Proc., 2022 14th Int. Conf. on Electronics, Computers and Artificial Intelligence (ECAI)*, 1–7. New York: IEEE.

Ukwen, D. O., and M. Karabatak. 2021. "Review of NLP-based systems in digital forensics and cybersecurity." *In Proc., 2021 9th Int. Symp. on Digital Forensics and Security (ISDFS)*, 1–9. New York: IEEE.

Van Dongen, S., and A. J. Enright. 2012. "Metric distances derived from cosine similarity and Pearson and Spearman correlations." Preprint, submitted August 14, 2012. http://arxiv.org/abs/1208.3145.

Walker, J. 2012. "Cyber security concerns for emergency management." In *Proc., Emergency Management*, edited by B. Eksioglu, 39–59. Rijeka, Croatia: InTech.

Walker, J., B. J. Williams, and G. W. Skelton. 2010. "Cyber security for emergency management." *In Proc., 2010 IEEE Int. Conf. on Technologies for Homeland Security (HST)*, 476–480. New York: IEEE.

Xiong, W., E. Legrand, O. Åberg, and R. R. Lagerström. 2022. "Cyber security threat modeling based on the MITRE Enterprise ATT& CK Matrix." *Software Syst. Model.* 21 (1): 157–177. https://doi.org/10.1007/s10270-021-00898-7.

Zhai, J., Y. Lou, and J. Gehrke. 2011. "ATLAS: A probabilistic algorithm for high dimensional similarity search." In *Proc., of the 2011 ACM SIGMOD Int. Conf. on Management of Data*, 997–1008. New York: Association for Computing Machinery.